

# FWD Code of Ethics and Business Conduct



# Introduction from CEO



At FWD, we're in the business of insurance. We aim to help our customers alleviate their financial worries and plan for their future. Every transaction that we undertake affects people's lives by enabling their financial sustainability, and with that knowledge comes great responsibility. To remind us that everything we do at FWD should be measured against high ethical standards, we adhere to **FWD's Code of Ethics and Business Conduct ("Code")**. This code is much more than just a set of rules though. It encompasses the principles that guide our day-to-day work and service as employees, appointed officers, directors or partners – such as agents or contractors – of a reputable and trusted insurer in Asia. It also addresses the expectations that we have of each other, as well as the high ethical standards that our customers and the public expect from us.

Simply put, we're building a culture of integrity where we **do the right things right**. For every situation we encounter, we remember this saying and use it to guide us. Whether you're new to FWD or have been with us for some time, I encourage you all to read and uphold this code, and always consider the impact of your actions on our customers, stakeholders and each other.

Reflecting our growing maturity as an organisation, we've expanded the code to more clearly articulate our strong governance and business ethics, the increased transparency of our decision-making, and the importance we attach to understanding the consequences of our actions on our stakeholders.

Please remember that you are not alone in the pursuit of ethical conduct – your colleagues, managers and leaders are always here to support you. If you have any questions or concerns about how to handle a situation, you can reach out to the resources outlined in this Code at any time, safe in the knowledge that your concerns and disclosures will be handled in the strictest confidence.

Our strong commitment to our Code will help us build an even better FWD, attracting the best talent, valuable partners and loyal customers.

Thank you for your support in helping us all to **do the right things right**.

Best regards,



**Huynh Thanh Phong**  
Group Chief Executive Officer FWD Group

# Table of contents

---

## FWD's guiding principles

---

### Introduction to our code

- Your personal commitment
  - Leadership responsibilities
  - Where to go for help
- 

## 1. Honesty and integrity

- Rejecting bribery and corruption
  - Political and charitable contributions
  - Gifts and hospitality
  - Conflicts of interest
  - Personal conflicts of interest
  - Corporate Opportunities
  - Structural conflicts of interest
  - Disclosing a conflict of interest
  - Respecting intellectual property
  - Gathering information about competitors properly
  - Respecting copyrights
-

---

## 2. Be informed and act responsibly

- Financial economic crime
- Recognising and avoiding money laundering
- Counter-terrorist financing
- Economic sanctions
- Know your customer
- Competing fairly in the marketplace
- Dividing markets
- Price fixing
- Insider dealing

---

## 3. Open and clear

- Conduct risk
  - Accuracy of records
  - Confidentiality and data privacy
  - Confidentiality of employee information
  - Confidentiality of customer information
  - Confidential information
  - Privacy and use of FWD systems and assets
  - Responding to external inquiries
  - Fair sales and marketing practices
  - Using social media responsibly
-

---

**4. Professionalism and respect**

- Keeping each other safe
- Harassment and discrimination
- Discrimination
- Harassment

---

**5. Socially and environmentally responsible**

- Environmental stewardship
  - Social responsibility
  - Human rights
  - No child nor forced labour
-

# FWD's guiding principles



# FWD's guiding principles

By Doing The Right Things Right, we can ensure FWD's continued success and uphold our reputation and brand. Regardless of our individual role in the company, whether we are directors, officers, managers, employees or FWD partners such as agents or contractors, we are expected to always Do The Right Things Right.

Underpinning this Code are our Five Guiding Business Principles: by embracing these principles on a daily basis, we can consistently Do The Right Things Right.

-  1 Honesty and integrity
-  2 Be informed and act responsibly
-  3 Open and clear
-  4 Professionalism and respect
-  5 Socially and environmentally responsible



1

## Honesty and integrity



**Acting with honesty and integrity means that you:**

- Comply with all governmental laws, rules and regulations, applicable to our business
- Deal with colleagues, customers, stakeholders and business partners with trust, respect and common courtesy
- Consider and do what is fair and ethical in all circumstances
- Refrain from putting personal interests above the company or our customers
- Handle actual, perceived, or potential conflicts of interest between personal and professional relationships in an ethical manner
- Do not tolerate dishonest or unethical behaviour from anyone.

2

## Be informed and act responsibly



**Being informed and acting responsibly means that you:**

- Carry out your duties with pride
- Are familiar with and understand the legal and compliance requirements of your role by completing all compliance training
- Take the time to be familiar with the policies and procedures that relate to your particular role and always act within your authority
- Meet and exceed company and managerial goals in a respectful and legal manner
- Refrain from abusing your position for personal gain.

3

## Open and clear



**Conducting your work in an open and clear manner means you:**

- Treat customers, partners and each other fairly
- Communicate transparently
- Present our products and services objectively, providing clients with a complete picture of the key features, benefits, exclusions and risks
- Never exaggerate or withhold information from customers, regulatory authorities or each other
- Provide full, accurate, timely and understandable reports and information to requesting parties when legally obligated to do so
- Promptly raise concerns about possible fraudulent or unlawful activity to your manager and to the Compliance department.

4

## Professionalism and respect



### Acting with professionalism and respect means you:

- Promote a workplace rich in diversity, where people of all backgrounds, race, colour, religion, gender, age and disabilities are accepted and embraced
- Encourage innovation, ideas and improved ways of doing our work, but never at the expense of doing the right thing by our customers and each other
- Do not tolerate discrimination, harassment, or bullying.
- Recognise and respect the importance of human rights which are an integral part of our business operations.

5

## Socially and environmentally responsible



### Being socially and environmentally responsible means you:

- Manage our business activities responsibly, to avoid negative impact on those around us and the environment
- Support our local communities, charities and causes that make a difference.

# Introduction to our Code



# Introduction to our Code

We have developed this Code as a source of guidance and to our commitment to building a strong risk culture based on a standard of ethical and transparent culture, including promoting sound overall governance, risk management and fair treatment of our customers, upholding human rights and supporting the sustainability of the communities in which we operate. It provides for principles for each of us to follow in the performance of our activities on behalf of FWD.

While no Code can cover every situation or challenge that we might encounter, we hope that the principles explained here will provide you with the guidance to make an informed decision in circumstances requiring ethical judgement.

This Code applies to all employees, officers, and directors of FWD as follows:

- 1 All FWD companies, affiliates, and subsidiaries
- 2 All FWD permanent, part-time, temporary and contract employees and contingent workers
- 3 All FWD directors, officers, supervisors and managers are expected to abide by the letter and spirit of this Code and any applicable contractual provisions when carrying out their obligations under their contracts with FWD.
- 4 All agents, distribution partners and third party business partners such as suppliers and contractors are also expected to abide by the standards set in this Code and to any applicable contractual provisions when performing services for or on behalf of FWD. We expect our third party business partners to act with the highest standards of professionalism and to ensure compliance with all applicable laws regulations while acting on our behalf, including without limitation, avoiding all forms of corruption and bribery, fair dealing with our customers, and protecting privacy of our customers.

Any employee, contingent worker, agent, distribution partner or third party business partner who believes that a situation may warrant an exception or waiver on the applicability of the Code should contact the Group Chief Compliance Officer.

Any waiver of compliance with the Code for executive officers or directors shall be approved only by the Board of Directors or to a Board Committee specifically designated to grant such approvals. Any such waiver of compliance granted by the Board shall be disclosed in accordance with applicable rules and regulations.

# Your personal commitment

Obeying the law because it is the right thing to do is the foundation in which the company's ethical standards are built. Thus, you are expected to be familiar and to comply with the Code and applicable laws and regulations in conducting the business of the company, including relevant securities laws and regulations.

You will be given access to this Code when you commence your employment or appointment with us and will be asked once per year to complete an online assessment and re-acknowledge your awareness of the Code and its contents. The Code needs to be read in conjunction with the more detailed policies at a Group or country level.

You are accountable and responsible for fully understanding and complying with the Code and applicable laws, regulations, internal policies and guidelines related to your daily work.

If you fail to comply with the standards contained in this Code, relevant laws, regulations and internal policies, you may be subject to disciplinary action up to and including dismissal, and possibly face legal penalties. This is why it is important to read the Code carefully and ensure that you understand its contents.



# Leadership responsibilities



Our leaders – directors, officers and managers, hold a special responsibility under this Code. They should set the example and create a positive environment for the promotion of these principles.



Leaders should discuss topics in this Code with employees, and make sure that employees understand how to Do The Right Things Right.



Most importantly, leaders should be ready to act promptly and consistently on reports of suspected violations. As a leader, if an employee reports potential misconduct to you or if you are aware that something is not right, you should be ready to manage the situation confidentially, take action, address the issue through proper procedure, and escalate the issue through the appropriate



Leaders should reach out to employees and communicate these principles regularly through:

- One-to-one meetings
- Team meetings
- Email
- An open door policy

# Where to go for help?

A culture of honesty includes our ability to speak up when we feel that something is wrong. We expect our employees, officers, directors and third party business partners to report any concerns if they observe or suspect misconduct within FWD.

You may choose to remain anonymous when you file your concern and we will take every effort to keep reports confidential and operate on a basis of non-retaliation. We will never retaliate against someone for making a disclosure to us and we do not tolerate retaliation against someone who makes a report in good faith.

## You can report violations or express concerns through a variety of avenues:

By phone – Speak Up Hotline (operated by an independent third party)



Cambodia – 2396 2515



China – 400-120-0253



Hong Kong – 800-903-375



Indonesia – 021-29223057



Japan – 0800-100-0081



Macau – 6262-5093



Malaysia – 01548770361



Philippines – 2-86263210



Singapore – 3158-7652



Thailand – 021056128



Vietnam – (028) 44581010



URL: Speak Up Online  
[www.fwd.com/SpeakUp](http://www.fwd.com/SpeakUp)



More information can be found in the FWD Whistleblower Policy

# Grievance reporting

To maintain good work relations and to establish a formal channel for employees to voice out and settle grievances such as incidents of discrimination and/or harassment, we adopt a robust mechanism for employees to report grievances and complaints. An employee is, however, encouraged to first consider raising and resolving any grievances informally.



More information can be found  
in the FWD Disciplinary and  
Grievance Policy



# 1. Honesty and integrity



# 1. Honesty and integrity



Acting with honesty and integrity means we follow all applicable governmental laws, rules and regulations and do what is fair and right, while never putting our personal interests before the company's goals. We are expected to act with common courtesy in all of our business dealings.



Our success is the result of the hard work and dedication of our people. We reject bribery and corruption as a way of building our business. We must not demand a bribe.



Anti-bribery and corruption laws also prohibit creation of inaccurate or false books and records and they require companies to develop and maintain adequate controls regarding corporate assets and accounting.



Bribery and corruption are prohibited by several laws applicable to FWD including: the Prevention of Bribery Ordinance (Hong Kong). You should also follow the anti-corruption laws and policy in place in your country.



Anti-bribery and corruption laws prohibit us from offering, giving or receiving or promising to offer, give, or receive anything of value to another person in order to retain business or otherwise gain an improper business advantage. This means that you cannot provide anything - including expensive gifts, cash, lavish meals or entertainment, excessively favourable discounts or terms, and similar items, to another person in order to retain business or otherwise gain an improper business advantage.

# Rejecting bribery and corruption



We also cannot make improper payments through business partners (such as agents) or other intermediaries.



We are prohibited from making facilitation payments, which are un-tariffed payments made to speed up, obtain or secure an obligation that is already owed to us. For example, if we are awaiting approval from a bank on a wire transfer of funds from a customer account, we cannot offer an improper payment (no matter the value) to speed up or secure that payment.



Many times, it can be difficult to identify who qualifies as a government official. Individuals holding public positions, such as heads of government departments and ministers, are not the only government officials we should be aware of. Individuals working for any entity owned or controlled in whole or in part by a government are also considered government officials and any improper payments to them are still violations of the law.



Our policy on bribery and corruption extends to both commercial entities (such as persons working for private businesses) and government officials. We should pay special attention to government officials because anti-bribery and corruption legislation often focuses on improper payments to them and the penalties for such payments can be severe.



It is our responsibility to determine whether parties involved in a transaction are government officials. If you have any questions, reach out to your manager or use the resources we have identified for more information.

# Political and charitable contributions



As a reputable insurance company in Asia, individuals may look to us to provide political or charitable contributions for a variety of causes. We cannot support these causes using FWD funds, resources or assets, or with reference to FWD's name without prior approval.



While contributing to political and charitable causes can be a worthy endeavour, a donation may be deemed as an underhanded bribe when given in a business setting or when related to an FWD transaction.



You may provide these types of contributions using your own funds and resources, without reference

# Am I doing the right thing?

**Question:** Sandra is working to set up a new office in The Philippines for FWD's operations. She is working with the local government to obtain the necessary permits and services to get everything in order. A government worker in charge of the utilities (water, electricity, telephones, etc.) says, "If you want this new office, you are going to need my help and I'm only going to do that if I get USD\$1,500 cash for my time." She is aware of certain set-up fees for the services but this seems suspicious. Sandra wants to get the new office set up soon but thinks this could be a bribe, what should she do?

**Answer:** Sandra should not make the payment and report the request from the government official to her manager and the Compliance department. The payment is highly suspicious as it was requested in cash, doesn't seem to be a normal fee and most likely qualifies as a facilitation payment. We want to get the job done but only if we Do The Right Things Right and paying bribes does not allow us to do that.

# Gifts and hospitality

Exchanging common business courtesies are an essential part of building strong working relationships with our business partners and customers. We should make sure that the gifts and entertainment we provide or receive do not amount to bribery or give the appearance that we are exchanging courtesies to gain any improper business advantage.

## Gifts and hospitality are permitted when they are:

- 1 Exchanged as part of the promotion or demonstration of one our products or services
- 2 Of nominal value (not lavish or overly expensive)
- 3 Infrequent
- 4 Unsolicited
- 5 Reasonable, ordinary, customary and lawful in the country or region where they occur
- 6 Not exclusive (commonly handed out to clients)

# Gifts and hospitality

(whether giving or receiving)

**Acceptable forms of gifts and hospitality include:**

<p>FWD promotional items For example, calendars, pens, coffee mugs, etc.</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>	
<p>Inexpensive souvenirs small gift items</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>	<p>Tickets to modestly priced events</p> <div style="text-align: center;"> </div>
<p>Inexpensive food items</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>	<p>Inexpensive meals and drinks</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>

**Prohibited forms of gifts and hospitality include:**

<p>Lavishly priced gifts</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>	<p>Expensive meals and drinks</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>
<p>Gifts / entertainment exchanged in relation to any business consideration or frequently with the same person or entity</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>	
<p>Attendance at “adult-only” establishments Such as gentlemen’s clubs, gambling venues, nightclubs and spas</p> <div style="display: flex; justify-content: space-around; align-items: center;"> </div>	

# Am I doing the right thing?

Use your best judgment when giving gifts or hospitality and follow the policy in place for your business

Think about whether the gift or hospitality is being exchanged to influence a person's decision or create a sense of obligation.

If yes, then that gift or hospitality could be a bribe or create the appearance of corruption and is against our Code and the law.

If refusing a gift or hospitality is not possible or feasible, or if refusal would be highly offensive to the person offering the benefit, accept the gift or entertainment and report the incident to the Compliance department.

In the case of gifts, you will also need to surrender the gift to the appropriate department in accordance with your local policy.



More information can be found in the FWD Anti-Bribery and Corruption Policy



# Am I doing the right thing?

**Question:** One of our brokers we have worked with for a long time has sent Stephen, a FWD employee, an expensive bottle of wine and a designer watch as a “thank you” for their many years of successful business. Stephen estimates that the total value of the gifts is about USD500. Can he keep these gifts?

**Answer:** No, Stephen should not accept the gifts. The gifts that are being offered to Stephen are lavish, not reasonable and could affect his decision making process about working with the business partner in the future. He should politely decline the gifts, inform the business partner that such gifts are against FWD’s policies and this Code and report the incident to the Compliance department.

**Question:** Linda, an FWD agent, has been working with one of her customers for many years and enjoys their good working relationship. The holidays are coming up and Linda wants to send her customer a card and a promotional calendar to thank her for her business and also as a way to promote the FWD brand throughout the year. Is it okay for Linda to send these to her client?

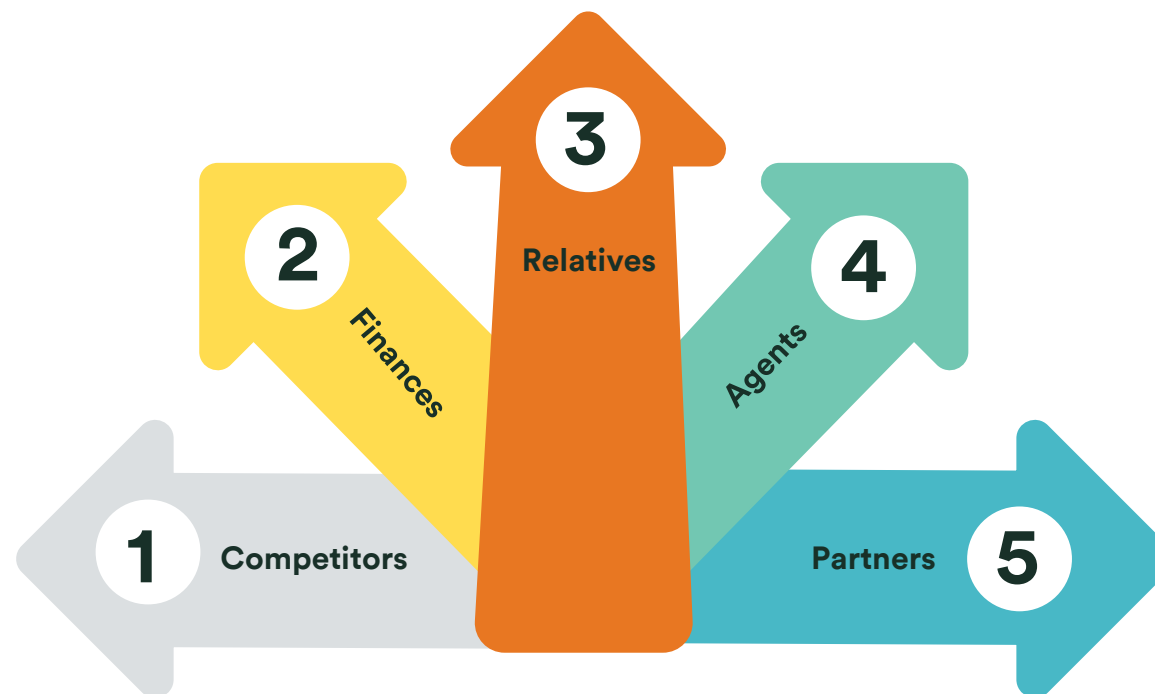
**Answer:** Yes, a simple card and promotional calendar are reasonable gifts that will promote our services and products. Providing gifts of low value around the holidays can be a good way to increase the visibility of the company and stay in touch with our valued customers.

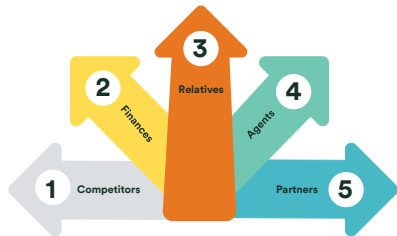
# Conflicts of interest

Fulfilling our clients' needs and meeting our stakeholders' expectations requires our full attention on a daily basis. To maintain our dedication, we need to manage our conflicts of interest to ensure that we act with integrity and in the best interest of our customers and shareholders.

A **conflict of interest** occurs when an individual's private interest interferes in any way - or even appears to interfere with the interests of the organisation as a whole. It may also occur in situations where the vested interest of two parties are at odds with each other, which may influence a party from making an informed and objective decision.

Whilst it is impossible to identify all potential conflict of interest situations, at FWD, a conflict can either be considered a Personal Conflicts of Interest or a Structural Conflicts of Interest.





## Personal conflicts of interest (individual vs customer / company)

Individual vs customer / company conflicts are considered personal conflicts of interest and may arise in situations where an employee, director, officer or contractor has a personal interest which may influence their objective judgment at the detriment of the customer or FWD.

### Competitors

Working for FWD’s competitors is a conflict of interest because your loyalty is divided between both companies and you may experience a clash of interests on a variety of matters.

In addition, working for a competitor limits your time to conduct work for FWD and creates a risk that business and products plans, or other confidential information could be revealed.

### Finances

Serving as a director of a competitor or holding significant financial interest in a competing organisation presents these same sorts of risks and could also qualify as a conflict of interest.

Additionally, when an employee, officer or director, or a member of his/her family receives improper personal benefit as a result of his/her position in the company, e.g., loans to or guarantees of such persons, etc.

### Relatives

Hiring relatives to work for FWD is not prohibited but relatives must be evaluated and considered under the same process and criteria as other candidates. If you have a relative that is interested in working for FWD, speak to the HR department about them and they will instruct you on the appropriate next steps.

### Agents

Steering business to specific agents or business partners can also be a conflict of interest, especially if the agent or business partner is related to you, has a relationship with you outside of work, or is a company you hold an interest in.

### Partners

If you know of an agent or business partner that FWD should be considered for an engagement or transaction, ensure that they undergo the same review process as every other potential third party.

## Corporate Opportunities

Corporate opportunities are business opportunities that a person encounters as an employee, officer or director of FWD. You cannot take these opportunities to enrich yourself personally or compete with FWD directly or indirectly, unless FWD has informed you that the company will not be pursuing the opportunity and has consented to you taking the opportunity.

# Structural conflicts of interest

Structural conflicts of interest arise in situations where there may be opposing interests between FWD and the customer, between FWD Group of companies, or between customers.

## Company vs customer

Company vs customer conflict of interest may arise in situations where FWD Group (or one of FWD Group companies) potentially benefits at the detriment of the customer. Below are some examples of potential conflicts in this category:

- Remunerations and incentive structures may influence sales force and sales staff to sell insurance products with higher commissions and incentives rather than based on the needs and suitability of the customer
- Managing participating funds to increase shareholder profits at the expense of policyholder interests
- FWD has a stake in a broker or financial advisor that distributes FWD products
- FWD receives from a party other than the customer an inducement in relation to a service provided to the customer other than the standard commission or fee for that service

## Company vs company

Company vs company conflict of interest may arise in situations where there is an intra-group conflict whereby FWD Group potentially benefits at the expense of another company within the FWD Group of companies or an affiliated company (or vice versa). Below are some examples of potential conflicts in this category:

- Investment manager invests in an asset which has an existing interest or stake by FWD Group or its majority shareholder
- FWD Group has a joint venture or stake in a company that is in direct competition with an existing BU
- Related/ connected party transaction

## Customer vs customer

Customer vs customer conflict of interest may arise in situations where a customer (or group of customers) has the potential to benefit at the expense of another customer. Below are some examples of potential conflicts in this category:

- Financial or other incentive (e.g. premium discounts and promotions) provided to a select cohort of customers
- Investment manager allocates trades for more than one customer and fund
- Different group of customers in par funds

# Structural conflicts of interest

## Management of structural conflicts of interest

Whilst FWD seeks to avoid and prevent perceived or actual structural conflicts of interest, it is acknowledged that in some instances, this will not always be possible. In these situations, Group Compliance will work with relevant parties to ensure that proposed controls and processes are fit for purpose to mitigate or reduce the risks that arise from the conflict, and that the conflict doesn't harm the fair treatment of our customers or the interests of our shareholders.

Examples of some controls and processes that could be implemented to manage conflicts are provided below (not an exhaustive list):



Controls to limit the exchange and use of information: Information barriers (“Chinese walls”) to prevent or restrict transfer of sensitive and confidential information between employees, FWD Group companies, or third parties involved in transactions where a conflict of interest may arise or could harm the interest of customers.



Organisational structures and segregation of duties: To ensure that potential conflicts of interest arising from the organisation of the company are prevented. These arrangements are usually defined in internal policies and procedures.



Controls over remunerations and other benefits: remuneration policies to prevent remunerations and other benefits accorded or received by FWD, employees, contractors, and sales force do not bring about conflicts of interest and promotes the interests of customers in a fair and transparent way.



Annual risk assessment and review of structural conflicts

# Disclosing a personal conflict of interest

If a situation or opportunity arises that could potentially cause a conflict of interest (whether potential or actual) to your role as a FWD employee, officer or director of FWD, you must disclose the conflict of interest to FWD Compliance.

Disclosing a potential conflict of interest does not necessarily mean that FWD will bar you from engaging in an activity. Rather, disclosure provides us with a chance to review the particular circumstances and communicate with you on whether you can safely pursue the situation or opportunity.

# Am I doing the right thing?

**Question:** We have a need for office cleaning services and I think my brother would be a great candidate for the job. He is a hard worker, has experience and is looking for a new job. However, I don't want to create a conflict of interest by suggesting him to the HR department, what should I do?

**Answer:** Hiring a family member is not always a conflict of interest. In fact, relying on personal referrals for hiring qualified partners is a valuable asset to FWD. However, before your brother can be hired you would need to remove yourself from the decision-making process so it doesn't appear to others that he is getting preferential treatment. He still needs to win the job based on the quality of his work and merit; not on personal relationships. Mention him to the HR department and they will take the next steps.



More information can be found in the FWD Conflicts of Interest Policy

# Respecting intellectual property

A part of doing business with integrity means respecting the intellectual property of others. Intellectual property relates to a variety of confidential information possessed by FWD competitors and external parties.

Intellectual property includes but is not limited to:



Business plans



Pricing information



Market research



Copyrighted information  
such as software, images,  
publications and notes

Respecting intellectual property rights means you should protect the intellectual property of others and only gather or use such intellectual property through legal and ethical means.



# Gathering information about competitors properly

We should only gather information about competitors through publicly available sources.



Competitor websites



Competitor annual reports



News, magazine and trade industry articles about the competitor



Web-based communities (such as internet forums and blogs)

## Am I doing the right thing?

If you happen to come into contact with a competitor's confidential information by way of a non-public source, you should not use the information. While it may seem beneficial to FWD, we are committed to only doing business honestly and with integrity.

If you have any questions on whether certain information you have can be used, please seek advice from the Compliance department.

# Respecting copyrights

In addition to gathering information properly, we should only access information and materials that we have a right to use.

For example, when putting marketing materials together, we can only use images that we have a license to use, such as pictures from our company image bank.

The same is true for the software that we use on our computers and music we use in commercials and videos.

If you have any questions regarding whether certain information or materials can be used for FWD business, please contact your manager.

# Am I doing the right thing?

**Question:** Mike is working on FWD's internal network when he notices a strange folder called "Songs and Programs". He opens the folder to find that there are hundreds of songs, images, movies and a few programs that appear to be downloaded without permission. What should Mike do?

**Answer:** Mike should let his manager and the Compliance department know what he found. It appears that someone has violated copyright laws by downloading materials without properly paying for them. At FWD, we only use materials (such as music, pictures and software) that are obtained legally and with permission of the copyright holders.

## 2. Be informed and act responsibly



## 2. Be informed and act responsibly



Being informed and acting responsibly means we do our jobs with pride, meet and exceed company and managerial goals in a respectful, legal and ethical manner, and refrain from abusing our position for personal gain. This also means that we don't need to try and know everything and be perfect but instead ask questions when we aren't sure what to do.

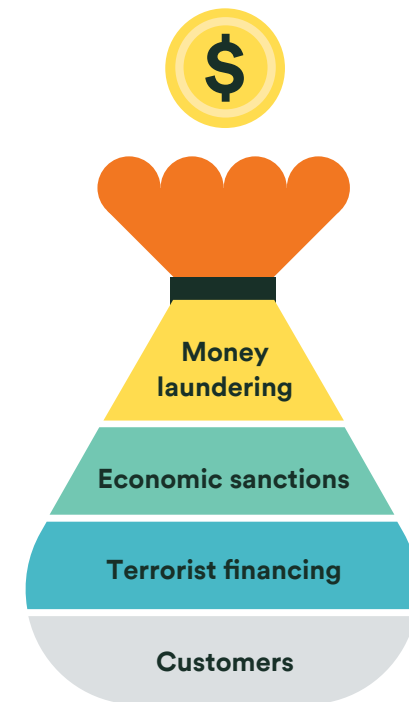
# Financial economic crime

At FWD, we specialise in insurance and financial products that can assist individuals, families and companies in many ways. Having a versatile set of products also means that we will attract a diverse group of customers.

While our customers are honest individuals and reputable organisations, and seek use of our products for sincere purposes, some potential customers may attempt to utilise our products and services for illegitimate reasons such as to launder money or finance terrorism.

In other instances, they may attempt to pay for our products or any associated fees (such as premiums) through wire transfers or other forms of payment made by sanctioned or blacklisted individuals or entities.

To guard against this we should conduct appropriate due diligence about a customer and make responsible decisions as to which customers we are comfortable working with. The following sections provide more information on these risk areas.



# Recognising and avoiding money laundering

Money laundering is the process of transferring illegally obtained money through legitimate avenues, in order to conceal the original source of the money. For example, someone profiting from illegal drug trafficking may place earnings in an investment scheme to hide the fact that the earnings were originally made from illegal drug sales.

As an insurance company, we need to ensure that our customers are not buying or investing in our products with illegally obtained funds as a way to launder money.

We must take time to learn who our customers are, how they have earned their wealth and acquire background information on why they are interested in our products.

Failure by us to identify customers, monitor customers' activities, and report suspicious or unusual activities could lead to FWD being held responsible for assisting in these crimes. Penalties for violation of anti-money laundering laws are severe.

# Counter-terrorist financing

Another risk we should be aware of is customers using our products and services to finance terrorist groups.

Governments are constantly checking to see how terrorists finance their schemes and as a result terrorists are always searching for new, underhanded ways to support their causes.

Investing in insurance products is one way terrorists covertly finance their causes. As a reputable Insurer, we do not want to serve such customers or be associated with them in any way.

Just as with money laundering, we need to learn about who our customers are. We should find out as much information as possible about who the insurance products and payouts are benefitting.



## Economic sanctions

FWD is committed to complying with the sanctions laws and regulations issued by international governing bodies as well as the laws and regulations of the countries in which we operate.

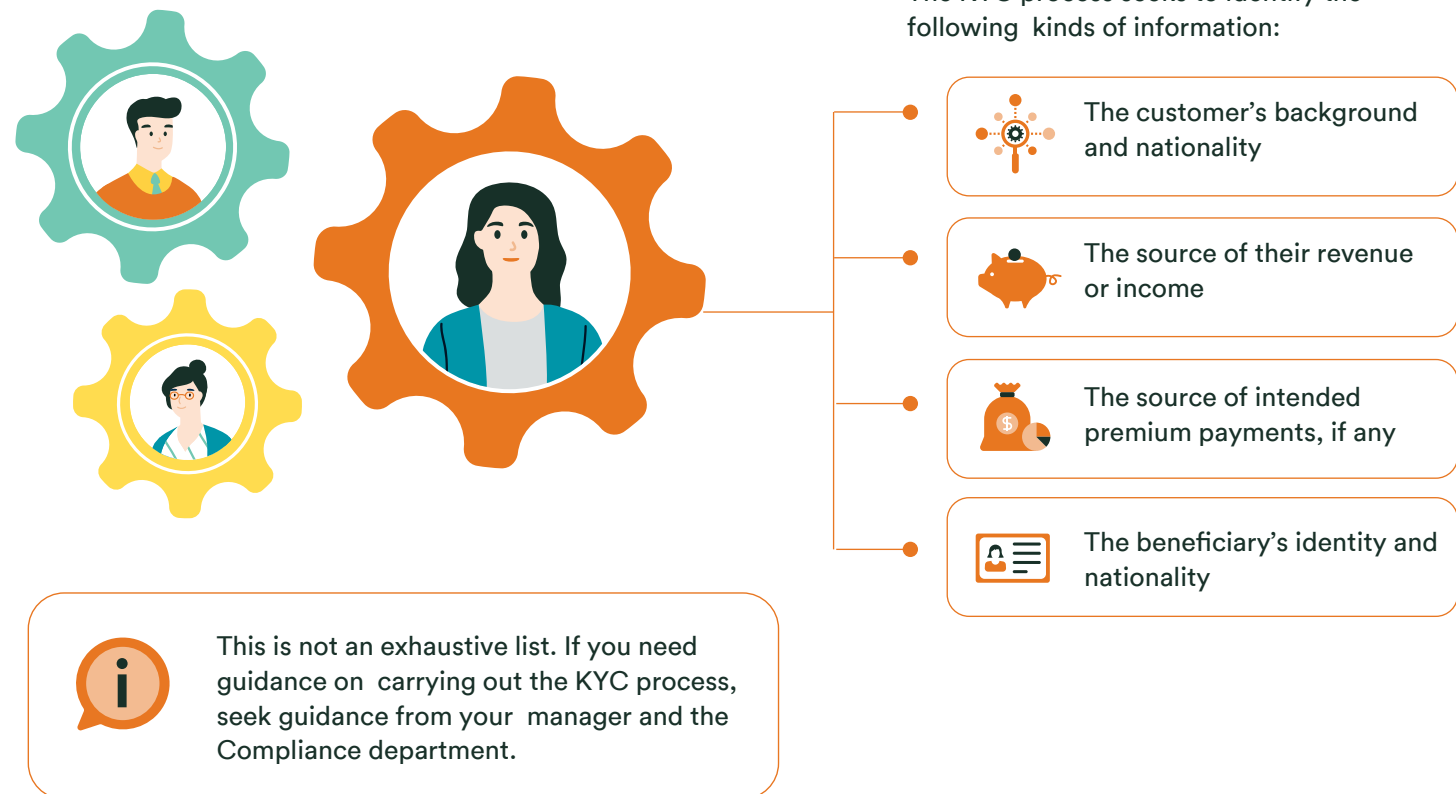
Beyond money laundering and terrorism concerns, we want to ensure that our customers, their payors, their intended beneficiaries and payees are not sanctioned or blacklisted entities.

It is our responsibility to determine whether customers or their related parties are sanctioned or on any applicable watchlists.

FWD prohibits business activities that it believes may violate applicable sanctions laws or the AML-CTF and Sanctions Policy. Dealing with individuals or entities subject of economic sanctions carries heavy penalties for FWD and our employees. If you have any doubt about whether a customer, supplier, business partner, beneficiary, etc. is sanctioned, you should escalate to the Group Chief Compliance Officer (AML Officer) immediately.

# Know your customer (KYC)

To learn more about our customers, their background, intended beneficiaries and other concerns, we employ a know-your-customer (KYC) process. The KYC process begins immediately after making contact with a prospective client and continues on throughout the sale.



# Am I doing the right thing?

**Question:** A customer has just purchased a high-value insurance policy. However, just a few days later, the customer asks for a refund and to cancel the sale. The customer also requests for the refund to be provided in the form of a cheque made out to his personal business and not to him (who initially made the purchase). Vanessa, the FWD agent who handles this customer, wants to help our customer but this request seems strange and she doesn't feel right. What should she do?

**Answer:** Vanessa should acknowledge her feelings that something is not quite right. The request of making a refund to a different company or individual should raise some red flags concerning money laundering. Before issuing any refund, Vanessa should talk to her manager and the Compliance department.



More information can be found in the FWD Anti-Money Laundering and Counter-Terrorism Financing and Sanctions Policy (AML and CTF and Sanctions Policy).

# Competing fairly in the marketplace

Our success depends on our hard work, knowledge and innovative products, rather than on engagement in unfair business practices, such as dividing markets and price fixing.

Competition laws and our policies prohibit us from engaging in anti-competitive activities that would harm customers and endanger our long-term success.

Violation of anti-competition laws carries severe penalties including prison time and large fines for any responsible employees.

## Dividing markets

Dividing markets involves agreeing with competitors to distribute markets to each company.

As part of this division, companies agree to exclusively deal in certain territories only, while refraining from doing business in other markets.

Dividing markets is against the law because it stops customers from having alternatives in their geographic region, often forcing them to pay higher prices.

# Price fixing

Price fixing involves an agreement among competitors to set prices for certain types of products or services.

Price fixing is against the law because customers expect prices to be determined by supply and demand and other market forces, rather than on agreements entered into by competitors.

**As part of Doing The Right Things Right, we should refrain from speaking to competitors about:**

- 1 Our business activities or plans
- 2 Customer data and insights
- 3 Our product pricing including premiums, deductibles, pay-outs, discounts and other price-related items
- 4 Any future products or marketing plans.

# Am I doing the right thing?

**Question:** While attending an insurance conference in Hong Kong, Jackie meets another agent from a competitor. At first, Jackie and the competitor talk about how much they are enjoying the conference, but then the competitor suddenly changes topics and says, “You know, we are wasting so much of our time and money trying to beat each other in Kowloon and New Territory. I think we could save ourselves some trouble if FWD focuses on Kowloon and my company focuses on New Territory; we’ll both make more money that way. What do you think?” How should Jackie react to this?

**Answer:** Jackie should let the competitor know that discussing market division is against FWD’s policies and make it clear that he does not agree to the competitor’s proposal. Jackie should end the conversation and report what happened to the Compliance department. The competitor was trying to engage FWD in anti-competitive practices and we need to document the incident to protect ourselves.



Seek advice from the Compliance department before initiating any discussions or meetings with competitors.

# Insider dealing

As employees of FWD, we may become aware of any material or price sensitive information about our company or other companies earlier than the public does. We cannot use such material or price sensitive information, before it is made known to the public for buying or selling securities to gain benefit. We also cannot engage in tipping off - using material or price-sensitive information to advise our friends, relatives or anyone else on trading decisions.

Information is “material” if a reasonable investor would consider such information important in deciding whether to buy, hold or sell securities. Material information is only considered “public” after it has been broadly released to the market such as by a press release. As an informed and responsible employees, we must check with the Compliance department to ensure that vital information you possess has been made public before trading in stocks.

Insider dealing or tipping can have serious consequences to FWD and the persons involved such as immediate termination, possible imprisonment and fines. Thus, if you have questions or any doubts as to the propriety of any transaction, e.g., purchase or sale of the company’s securities or other company’s, seek advice from the Group General Counsel, Group Chief Compliance Officer or their designated officers before undertaking the said transaction.



More information can be found in the FWD Insider Dealing and Market Misconduct Policy.

# 3. Open and clear





## Open and clear



Conducting our work in an open and clear manner is more than just being honest. It includes treating customers, partners and each other fairly and being transparent in our business dealings.

Every day, we present our products and services objectively, never exaggerate or withhold information from customers, regulatory authorities or from each other. We take it upon ourselves to promptly report concerns or potential violations.

# Conduct Risk

At FWD, we define Conduct Risk as losses arising or adverse consequences due to conducting insurance business in a way that does not ensure the fair treatment of customers, fair outcomes, or results in harm to customers.

Managing Conduct Risk is an important backbone to our culture and customer experience as it helps us identify and manage risks that could jeopardise delivering fair outcomes for our customers.

We all have a responsibility to manage conduct risk as we all create and influence and make decisions to ensure the fair treatment of our customers throughout the customer's journey.

Examples of Conduct Risk:

1

Recommending a product that's not fully aligned to our customers' reasonable expectations at the point of sale

2


Sales and distribution communications or practices that are unclear, unfair or potentially misleading


3

Any unnecessarily complicated claims, complaints or cancellation process

# Conduct risk

FWD customer journey examples

<b>Product and pricing</b> 	“Products which meet customer needs and are priced fairly”
<b>Marketing and distrib.</b> 	“Customer facing materials which are clear, fair and unambiguous”
<b>Sales / renewals</b> 	“Sales and distribution practices which protect the interests of customers”
<b>Admin and servicing</b> 	“Servicing which is fairly priced, straightforward and timely”
<b>Claims</b> 	“Claims are settled quickly and declinatures are clearly explained”
<b>Complaints</b> 	“Complaints resolutions are clearly communicated and reached on a timely basis”
<b>Cancellations</b> 	“Cancellations are straightforward and not highly priced”

 More information can be found in the FWD Treating Customers Fairly (TCF) Policy

# Accuracy of records

By keeping accurate records, we protect our company's reputation as a trusted insurance partner.

Maintaining accurate records helps to:

- Identify improper transactions
- Confirm that transactions with customers are carried out according to our standards
- Meet industry regulations on proper accounting practices
- Maintain a clear and transparent vision of our financial status
- Forecast future opportunities more clearly
- Meet internal and external audit review procedures.

We must also properly manage our records. Record management is important to meet industry regulations and to comply with the requests of internal and external auditors, who can help to ensure that our company is meeting our financial goals.

The most important part of maintaining accurate records is to follow our approved accounting procedures. This includes submitting accurate documentation related to our job duties (such as time sheets and expense reports) and records of dealings with customers.

Where disclosures to regulatory bodies are required to be made or in other public communications made by the company, relevant employees and officers shall ensure that such reports and documents are full, fair, accurate, timely and understandable, including accurate financial and accounting data, where applicable.

We must not knowingly falsify information, misrepresent or omit material facts necessary to avoid misleading our independent auditors or investors. We must also never be dishonest or deceptive in maintaining FWD records, or otherwise attempt to mislead FWD's management, regulators or shareholders, or coerce, manipulate, mislead or fraudulently influence our independent auditors in the performance of their audit or review of FWD's financial statements.

## Am I doing the right thing?

**Question:** I am nearing the end of a sales quarter and have already met my quota. I've had a number of sales come in at the last week of the quarter and I'm thinking about waiting until next week to process them to get a head start on next quarter's quota. In the end, FWD still gets the business so I don't think I'm doing anything wrong. Is this okay?

**Answer:** No, this is not okay. All records and transactions need to be properly recorded when they actually occurred. Waiting to process the sales will not create an accurate picture of FWD's financial status.

**Question:** Irene is a manager and is going through some expense reports submitted by her employees. During her review, Irene sees an item on a report for "Conference fees in Hong Kong" for a conference that she knows the employee did not attend. Additionally, there are other items related to the conference without any receipts. It appears that one of her employees is trying to commit expense report fraud. What should she do?

**Answer:** Irene should first contact her employee to determine if the reimbursement for conference fees was made in error. Everyone makes mistakes from time to time and this could simply be a miscommunication. However, if the employee continues to insist that the fees and request for reimbursement are genuine, further steps should be taken to confirm if the expenses are fraudulent or not. Additionally, we should be careful when submitting expense reports to ensure accuracy.

# Confidentiality and data privacy

A key to our success is protecting confidential information. As FWD employees, officers and directors, we are expected to maintain the confidentiality of information entrusted to us by the company and our customers, unless disclosure of such is authorised or legally mandated. By protecting such information and our data, we can maintain our competitiveness in the market and demonstrate to customers that we are a trustworthy and valuable partner. We take great care in protecting essential information.



## Confidentiality of employee information

We have access to private, personal information of FWD employees, including contact information and compensation details. In accordance with all applicable data privacy laws, we only release personal information if legally required to do so by government authorities, such as for tax purposes.

As an employee of FWD, you may also have access to employee personal information, such as names, addresses, email, credit card, bank details and other information. You are required to treat this information confidentially during your employment with us and afterwards.






## Confidentiality of customer information

At FWD, we understand the close relationships we must build with our customers to provide products that can truly enrich their lives.

We also understand that through our role, we will come into possession of various kinds of personal information. We take great pride in preserving the confidentiality of this information to maintain client trust and to comply with all applicable data privacy laws.

### Confidential information

includes all non-public information that might be of use to competitors, or harmful to FWD and our customers, if disclosed. Thus:

-  Should only be used for company purposes;
-  Should only be shared with colleagues on a need-to-know basis;
-  Should never be shared with anyone outside of FWD (unless the Compliance department permits you to share the information, such as when a Non-Disclosure Agreement is in place or when required by a government authority).



More information can be found in the FWD Data Privacy Policy

## Privacy and use of FWD systems and assets

All information entered into by employees using our systems or otherwise stored on our systems can be accessed and viewed by FWD. However, we respect our employees' privacy and do not unnecessarily monitor all employee action. Information may be accessed or reviewed should a need arise in accordance with local laws.

Company systems and assets should only be used for legitimate business purposes. Theft, carelessness and waste have an impact on the company's profitability. Thus, all FWD employees, officers and directors should protect FWD's assets and ensure its efficient use. Any suspected incident of fraud or theft should be reported immediately.

## Responding to external inquiries

There may be instances when outside parties, like government authorities or the media, request information. We are prepared to comply with requests by government authorities when legally required to do so. If you are presented with a request by a government authority for any information, please contact the Compliance department to determine whether we are legally required to release the requested information.

We also respond to media inquiries to keep the public informed about FWD's activities. Only FWD employees approved by our Brand & Communications department may speak on the company's behalf to media outlets. If a media outlet (such as a TV or newspaper reporter) makes an inquiry of you, please contact our Brand & Communications department to determine the proper next steps.



More information can be found in the FWD Communications Policy and FWD Inside Information Disclosure Policy



# Fair sales and marketing practices



Our products have the power to change lives for the better. We should always present our products accurately and take the time to describe the key features, benefits, exclusions and risks to our customers so that they are able to make informed decisions.

All agents working to sell our products must provide clear, adequate and not misleading full and complete information to customers. Managers should review the sales practices of all employees and agents to ensure that communications regarding our products are truthful and accurate.

We always accurately present products to customers, not just during sales interactions, but also through the use of approved marketing materials. Misrepresentations, whether intentional or not, are not permitted.

To put your best foot forward you should spend time thoroughly understanding our products. When you have questions or need more information, seek out information from your manager.

## Am I doing the right thing?

**Question:** Bruce has recently been hired as an agent for FWD. One of his co-workers, Craig, has offered to let Bruce listen to some of his sales calls. During the sales calls, it seems to Bruce that Craig is not being completely truthful with his clients. Craig often uses jargon and complex terms to describe products. What should Bruce do?

**Answer:** Bruce must raise his concerns with Craig and their manager to address the issue. Craig must be transparent and honest during sales calls and use clear and layman language to describe all products and services.

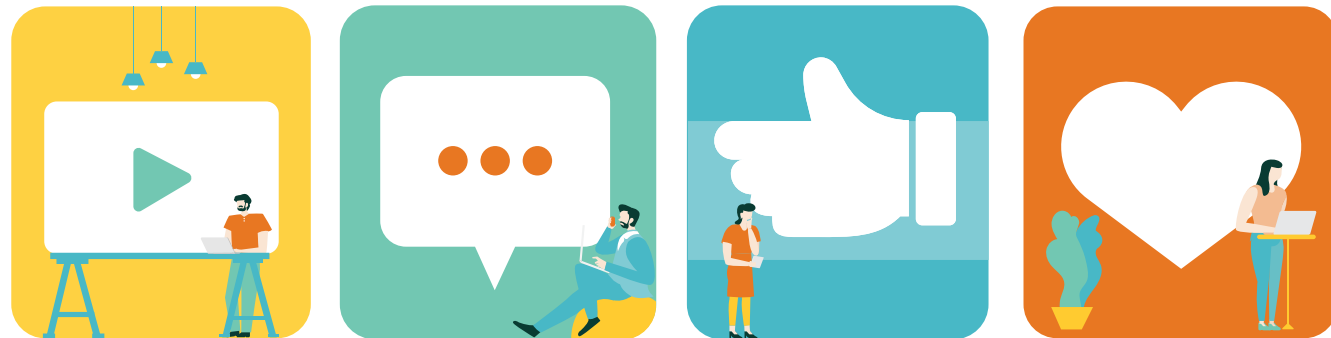
Craig is not living up to our Code by describing our offerings in a way that is difficult for customers to understand. When we market and sell our products, we need to simply and accurately describe what we are offering along with the potential risks involved.

When in doubt, both Bruce and Craig must immediately seek clarification on the appropriate way of presenting any products and services with their manager and/or agency leader.

# Using social media responsibly

We may be able to utilise certain social media platforms to promote or raise awareness of FWD's products and services. The Marketing & Communication department, in conjunction with the Compliance department, will advise us on who can communicate with social media on behalf of FWD.

When we use social media we should be respectful of FWD and each other. We must never reveal confidential information through social media, or present the official opinions of the company without prior approval. All of the guidelines about confidential information apply when using social media. If you have questions, please seek advice from your manager and the Compliance department.



## Am I doing the right thing?

**Question:** I like to browse various websites about insurance and investing. While looking at one site, I see that someone has posted some information about FWD's products and services that is not accurate. Is it okay that I tell people on the website that I work for FWD and give them the accurate information?

**Answer:** No. While your intentions are good, only certain people at FWD are authorised to speak or make posts online on behalf of FWD. Using social media is complex and new to many of us. If you have any questions, talk with your manager.



More information can be found in the  
FWD Social Media Policy

## 4. Professionalism and respect



# Professionalism and respect



Acting with professionalism and respect is an important part of working for an international company. We value the welfare of our colleagues and customers, and genuinely strive for our company's collective success.

We can achieve these goals by maintaining a safe and healthy workplace, promoting diversity and inclusion, being open to new ideas and being able to speak up promptly and report any misconduct.

## Keeping each other safe

The safety and health of our employees is one of our top concerns. We provide a strong work environment to promote employee safety and well-being. Employees are required to follow our safety policies to help maintain this environment.

Please be aware of your surroundings at all times. If you have a concern regarding our work premises, think something can be improved or made safer or are worried about your or another employee's health, please let us know. We are receptive to feedback and take all reports seriously.

We expect employees to be sober while on work premises or when carrying out work engagements in off-site locations. You must not be under the influence of alcohol or drugs (regardless of whether they are legal or not) while conducting FWD business.

At company social events or during off-site meetings with customers, alcohol may be consumed in moderation and in reasonable amounts.

If you have any questions regarding our safety policy, please speak to your manager.



More information can be found in the FWD Staff Handbook.

# Harassment and discrimination

Consistent with our core as an international company that is diverse and inclusive, we expect professionalism and respect where we treat each other fairly and embrace our international culture and organisational values. All employees (including directors), contractors at all levels and distribution partners (including agents and brokers) are expected to promote a workplace where all people are valued.

At the same time, we do not tolerate any form of discrimination, harassment or bullying towards each other, our customers, business partners, agents or candidates interested in joining FWD.

## Discrimination

Discrimination means treating someone differently due to their characteristics, including without limitation, race, colour, nationality, ethnicity, gender, sexual orientation, marital status, medical or physical condition or disability or some other unique characteristic. At FWD, we embrace the unique qualities of all of our employees and customers, and treat each other with respect at all times.

We do not discriminate during hiring decisions and build our workforce based on the merit of each candidate.



More information can be found in the FWD Anti-Harassment and Non-Discrimination Policy



# Harassment

Harassment includes verbal, physical or sexual behaviour towards another person which causes them discomfort, intimidates or marginalises them. Any harassment, whether verbal, physical or environmental, is strictly prohibited by FWD and in some FWD markets, harassment on certain grounds may also be unlawful

The standards of a reasonable person are applied in determining whether harassment has occurred, i.e., any unwelcome behaviour in circumstances where a reasonable person would have anticipated that the harassed person would be offended, humiliated and/or intimidated. In determining whether a person carried out harassment, it is irrelevant whether or not that person is aware of the harassment, or whether or not it was intentional.

## Bullying

Typical bullying conduct in the workplace includes repeatedly making derogatory or insulting remarks, intentional targeted isolation, serious or repeated verbal or physical conduct that could reasonably be considered threatening, intimidating or humiliating; and intentionally sabotaging or undermining another's work performance.

The presence of bullying behaviours directly and negatively impacts workplace safety and will not be tolerated at FWD.

## Prevention

All FWD employees (including directors), contractors at all levels and distribution partners (including agents and brokers) have the responsibility to behave in a manner which is non-discriminatory, appropriate, and which respects the rights and psychological safety of others. There is an expectation that to contribute towards an environment of trust and respect, we will all conduct ourselves in a manner which does not cause offence or is not likely to be perceived as offensive by others and if we see behaviour not aligned with this policy, we are obliged to follow-up.

FWD will take all reasonable steps to prevent discrimination, harassment and bullying.

In our commitment to workplace respect, inclusion, physical and psychological safety, FWD offers both informal and formal resolution options for people to raise discrimination, harassment or bullying concerns via Compliance, your manager, Human Resources or our Whistleblower process.

All reports made via the avenues above and any investigation process will be held confidentially. At FWD, we do not accept or allow retaliation against any person making a disclosure in good faith. We will not tolerate intimidation or victimisation of any employee who reports a concern or assists in the investigation about discrimination, harassment or bullying.

## Am I doing the right thing?

**Question:** I am at my desk working when I hear a couple of my co-workers talking about Maria, a new employee we hired in the marketing department. I hear them say, “Maria is too old to understand what we are trying to do. She is not from Asia, so she doesn’t understand how to make a plan that appeals to our customers. We need to stop giving her projects so she takes the hint that she’s not wanted at FWD”. What should I do?

**Answer:** You should say something to your manager. Our policy on diversity allows us to include many different perspectives on how best to get a job done. Your co-workers in this situation are likely discriminating against Maria based on her age and country of origin. Discrimination hurts us all and we need to ensure that it is not tolerated at FWD. More information can be found in the Anti-Harassment and Non-Discrimination Policy and the FWD Whistleblower Policy.

## 5. Socially and environmentally responsible



# Socially and environmentally responsible



Being socially and environmentally responsible with a commitment to respect and promote human rights is expected of everyone working for a reputable company like FWD. It means we manage our business activities responsibly, avoid negative impact on people and the environment, reach out to the community to give back and support noble and just causes.

# Environmental stewardship

We should ensure that our work also has a positive impact on the environment and at the minimum, meet local and international environmental regulations. We should also consider the environmental impact of our operations and investments.



# Social responsibility

At FWD, we believe everyone matters and supporting the communities around us is one of our core values.

In order to positively contribute to our communities, we should stay aware of relevant issues affecting people and society. Our company may organise events such as hikes, walks and charity drives to fundraise for important issues. We encourage you to join these events.

We may support or engage with non-government organisations (NGOs) using FWD's name or resources. As discussed earlier, we only support these causes if approved by our leadership. You may personally support specific causes using your own funds and resources, and without reference to FWD's name, as long as your intention is sincere and never to gain a business advantage for our company.



More information can be found in the FWD Community Care Guidelines.

# Human rights

We are committed to the promotion of human rights. This means that:

- We promote diversity and inclusion in our workplace
- We do not tolerate discrimination harassment of any kind
- We provide a safe and healthy work environment
- We respect and protect our employees' labour rights, such as entitlements to wages, leave and other benefits, work hours arrangement and continuing training and career development
- We prohibit the use of child labour and forced labour
- We respect the freedom of our employees to express their personal opinions subject to the need to protect our reputation and to maintain an inclusive working-environment
- We provide an effective mechanism for reporting grievances and whistleblowing without fear of retaliation
- We protect data privacy of our customers and employees
- We do not work with customers, agents or business partners that are known human rights violators
- We recognise our employees' right to organise as they see fit, as long as organisation is allowed locally and does not disrupt our ability to carry out work for FWD.



More information can be found in the  
FWD Human Rights Guidelines



## No child nor forced labour

We do not tolerate the use of child or forced labour, and/or exploitation of children in any of our business operations and we strictly adhere to our principles that an employee or contractor should have the right to leave the work premises after completing the standard workday and to terminate employment after giving reasonable notice.

We support, follow and abide by labour laws and regulations where we conduct business, including those that address child labour and forced labour. We uphold the elimination of all forms of child labour and forced labour and prohibit the use of under-age and compulsory labour.

# Remember to always Do the Right Things Right!

You can report violations or express concerns through a variety of avenues:

By phone – Speak Up Hotline (operated by an independent third party)



Cambodia – 2396 2515



China – 400-120-0253



Hong Kong – 800-903-375



Indonesia – 021-29223057



Japan – 0800-100-0081



Macau – 6262-5093



Malaysia – 01548770361



Philippines – 2-86263210



Singapore – 3158-7652



Thailand – 021056128



Vietnam – (028) 44581010



URL: Speak Up Online  
[www.fwd.com/SpeakUp](http://www.fwd.com/SpeakUp)

C2 - Internal



# Anti-Money Laundering/Counter Terrorist Financing and Sanctions Policy

Document ID	KH-COM-PO-0001	Document type	Policy
Issued by / Owner	Chief Corporate Governance Officer	Approved by	Board of Directors
Target audience	All managements, employees, contingent workers, and contractors at all levels		
Document status	In-effect	Date last approved	16 August 2023

## Document approval history

Version	Date approved	Description
1.0	18 August 2021	First Version
2.0	10 Sep 2021	<p>Advised by CAFIU to revise on section 5.2</p> <ul style="list-style-type: none"> <li>- enables timely identification of reportable transactions including Cash Transaction Report and Suspicious Transaction Report to the Cambodia Financial Intelligent Unit (CAFIU) and ensures accurate filing of required reports; and</li> <li>- is to act as the main point of co-ordination with the CAFIU and other competent authorities.</li> </ul>
2.1	3 August 2022	Annual Review and Update
2.2	16 August 2023	Annual Review and Update



## Contents

1.	Background .....	4
1.1	What is the Nature of Money Laundering and Terrorist Financing? .....	4
2.	Objectives .....	4
3.	Scope .....	5
4.	Compliance Principles of AML/CTF and Sanctions .....	5
5.	Roles & Responsibilities.....	6
5.1	Board of Directors .....	6
5.2	Senior Management .....	7
5.3	Compliance Department .....	8
5.4	Employees and Intermediaries.....	9
5.5	Human Resources.....	9
6.	Three Lines of Defence .....	10
6.1	First Line of Defence.....	10
6.2	Second Line of Defence.....	10
6.3	Third Line of Defence .....	10
7.	Compliance Risk Management .....	11
7.1	Customer and Third-Party Due Diligence .....	11
7.2	Simplified Customer Due Diligence.....	12
7.3	Enhanced Customer Due Diligence .....	13
7.4	Reliance on Third Parties .....	14
7.5	Due Diligence on Third Parties .....	15
7.6	On-going monitoring of customers.....	15
8	Monitoring of Customers and Transactions .....	15
9	Recognising and Reporting Suspicious Activities.....	16
9.3	Reporting Suspicious Activities .....	16
9.4	Recognising Suspicious Activities .....	16
10	Record Keeping.....	17
11	Training and Awareness .....	17
12	High-risk and Other Monitored Jurisdictions .....	18
13	Sanctions.....	18
13.1	Sanctions and Its Associated Risks.....	18
13.2	Proliferation Financing .....	19
13.3	Insulation of US Persons and European Union Persons .....	20
14	Screening .....	20
15	Transparency .....	20
16	Reporting .....	21
17	Definitions.....	21
18	Sources of Further Information .....	23
18.1	Financial Action Task Force (FATF) .....	23
18.2	International Association of Insurance Supervisors (IAIS).....	23
18.3	Transparency International.....	23

## 1. Background

### 1.1 What is the Nature of Money Laundering and Terrorist Financing?

Money laundering is the act of concealing the criminal nature of any proceeds obtained from an unlawful activity with the intention of making it not to appear to be proceeds from such activity. Three common stages in laundering of money are:

**PLACEMENT:** The physical disposal of cash proceeds derived from unlawful activities.

**LAYERING:** Separating the unlawful proceeds from its original source by creating layers of transactions designed to disguise the source of the money and audit trail.

**INTEGRATION:** Integrate the laundered proceeds into the financial system so as to appear to be from legitimate business activities.

Terrorist financing is the provision or collection, by any means, directly or indirectly, of any property with the intention that the property be used, or knowing that the property will be used, to facilitate or carry out terrorist acts regardless of whether the property involved in the transaction were proceeds of unlawful activity or were derived from lawful activity. There is often a need to disguise links between terrorists or terrorist organizations and their funding sources.

FWD (“FWD”) is fully committed to complying with applicable legislation and regulations on anti-money laundering and counter terrorist financing (“AML/CTF”) as well as Sanctions regulations in countries where it operates. As a reputable insurer and being an integral part of the financial system, FWD is vulnerable to money laundering, terrorist financing and sanctions activities where its products and/or services could be used as a vehicle for laundering money or financing terrorism. Failure to detect or combat money laundering, terrorist financing and sanctions restrictions may expose FWD and its employees to criminal charges, including fines and imprisonment, and may cause serious reputational damage to FWD.

## 2. Objectives

FWD views compliance with AML/CTF and Sanctions standards as important as its business. The Anti-Money Laundering/Counter Terrorist Financing and Sanctions Policy (“this Policy”) aims to:

- ensure that FWD, its executives, employees, and sales intermediaries (e.g. agents) who act on behalf of the FWD entities, understand the AML/CTF and Sanctions requirements and are aware of their roles and responsibilities in achieving compliance;

- set and align the AML/CTF and Sanctions compliance objectives, corporate compliance governance framework, compliance control design, implementation and monitoring system in order to ensure consistent implementation of AML/CTF and Sanctions controls within FWD;
- identify and define major AML/CTF and Sanctions compliance requirements;
- define procedures for making AML/CTF and Sanctions risk decisions; and
- define information flows for reporting AML/CTF and Sanctions suspicious activities

This Policy has been prepared with reference to current Cambodia Financial Intelligent Unit (“CAFIU”) guidance and applicable regulations, and approved by the Board of Directors (“BOD”). It should be reviewed from time to time to keep abreast with applicable legislative and regulatory requirements. Any material impact to existing local policies and procedures should be taken into account in the update of this Policy.

### 3. Scope

This Policy establishes the general framework as well as setting the minimum standard to which FWD adheres to. It is applicable to entities controlled through management influence by FWD and which fall within the remits of relevant AML/CTF and Sanctions legislation and regulations. If there is any conflict between this Policy against local legislation and regulations, local legislation and regulations must be followed.

This Policy applies to all FWD entities, business units and subsidiaries of the Company. It should be read in conjunction with other applicable policies, standards, procedures and guidelines.

### 4. Compliance Principles of AML/CTF and Sanctions

This Policy is established on the following agreed AML/CTF and Sanctions principles:

- Ensuring the FWD AML/CTF and Sanctions compliance is everyone’s responsibility. All relevant company executives, employees and sales intermediaries should receive relevant AML/CTF and Sanctions training to equip them with sufficient knowledge to discharge their responsibilities;
- FWD, its entities, employees and sales intermediaries are strictly prohibited from directing, engaging or assisting any policyholder (e.g. customer) or payee to avoid fully disclosing Customer Due Diligence (“CDD”)/Know Your Customer (“KYC”) details or to avoid AML/CTF

and Sanctions liability. FWD's sales intermediaries and operating staff are prohibited from giving legal advice to a customer in preparing their self-declaration forms;

- CDD should be properly conducted for all new and pre-existing customers. New policy application should not be accepted until CDD is complete, with no outstanding, pending, or missing requested documents or information.
- 'Reason to know' principle should be applied throughout the customer policy/contract life in reviewing customer submitted documents and information;
- Overall company's AML/CTF and Sanctions governance, documentation, record keeping, and reporting compliance should be overseen and monitored by the Compliance Officer/Money Laundering Reporting Officer ("MLRO");
- FWD must have operational Policies and Procedures as well as internal control system in place to outline and ensure on-going AML/CTF and Sanctions compliance;
- The Three Lines of Defence risk management control framework should be in place and operating effectively for AML/CTF and Sanctions; and
- If FWD rely on third parties (such as distributors or bancassurance partners) to comply with AML/CTF and Sanctions obligations, the Company itself remains ultimately responsible for the AML/CTF and Sanctions compliance.

## 5. Roles & Responsibilities

The BOD is accountable for approval of the Policy and directs the development and maintenance of minimum standards, guidelines and procedures pertaining to this Policy, but has delegated the day-to-day responsibility for overseeing and implementation of this Policy to MLRO.

### 5.1 Board of Directors

The Board of Directors ("Board") has continuous oversight of the overall AML/CTF and Sanctions program. By demonstrating its commitment in establishing an effective internal controls system in compliance with local legislation and related regulatory guidelines on AML/CTF and Sanctions, the Board plays a critical role in setting an AML/CTF and Sanctions compliant culture. To fulfil its duties, the Board must be kept informed of timely information and at a minimum provided with a quarterly report on AML/CTF and Sanctions from the Compliance team.



## 5.2 Senior Management

Senior management has ultimate responsibility for ensuring the existence and an operationally effective AML/CTF and Sanctions compliance governance structure including suspicious activity monitoring and reporting. Senior management must also ensure adherence to implementation of this Policy and in particular for:

- incorporating the requirements of this Policy into procedures as applicable;
- seeking compliance with this Policy and applicable laws and regulations;
- requesting advice from the MLRO on any exception, deviation and waiver requests;
- putting in place adequate control and approval mechanism for higher risk customers, transactions and products, as necessary, such as imposing transaction limits or management approvals; and
- designating an individual or individuals at senior management level within the Compliance function, preferably the local Chief Corporate Governance Officer or to be agreed with Group Compliance, as the Money Laundering Reporting Officer (“MLRO”) responsible for managing AML/CTF and Sanctions risk management and compliance, who:
  - is/are independent of the activities being monitored;
  - has timely and unrestricted access to customer documents and any relevant information;
  - enables timely identification of reportable transactions<sup>1</sup> including Cash Transaction Report<sup>2</sup> and Suspicious Transaction Report to the CAFIU and ensures accurate filing of required reports; and
  - is to act as the main point of co-ordination with the CAFIU and other competent authorities.
  
- Detail of role and responsibilities of MLRO is to comply with Prakas on Anti-Money Laundering and Combating the Financing of Terrorism relating to all Reporting Entities not regulated by the National Bank of Cambodia (December 21, 2010) as below:

---

<sup>1</sup> Reportable transaction is to be determined by the appointed MLRO.

<sup>2</sup> Cash Transaction Report refers to the report to file to CAFIU for any payment transactions that have been made/received in real cash.

- Implementation of the policies for AML/CFT measures;
- the appropriate AML/CFT procedures including customer acceptance policy, customer due diligence, record keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
- regular assessment of the AML/CFT mechanisms to ensure that the mechanisms are sufficient to address the changing trends;
- the channel of communication from the respective employees to the compliance officer is secured and that any information is kept confidential;
- compliance with the AML/CFT legal and regulatory requirements;
- all employees are aware of AML/CFT measures including policies, control mechanisms and channels of reporting to ensure the effectiveness of such measures;
- the identification of money laundering and financing of terrorism risks associated with new products or services or arising from the reporting entity's operational changes, including the introduction of new technology and processes.

### 5.3 Compliance Department

Compliance function has oversight responsibility of all activities relating to prevention and detection of money laundering and terrorist financing including:

- informing senior management of emerging AML/CTF and Sanctions risks and compliance initiatives, as well as identified compliance deficiencies and corrective action taken;
- conducting annual risk assessment and monitoring of controls in accordance with the Policy and Procedures;
- providing appropriate training to all relevant employees, in particular adequate level of training for employees that complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of FWD's AML/CTF and Sanctions program;
- generating the information needed by senior management to obtain an overview with respect to risk management and compliance as dictated by the Compliance Charter & Framework;
- establishing an appropriate procedure for escalation of potential AML/CTF and Sanctions cases;

- taking appropriate action when breaches of this Policy are identified;
- making periodic reports to Group Compliance, Senior Management and Audit Committee on its AML/CTF and Sanctions activities;
- conducting an annual review of the AML-CTF and Sanctions policy, procedures and guidelines to ensure continuing compliance with local and Group AML-CTF and Sanctions requirements; and
- monitoring and reviewing the effectiveness and appropriateness of its AML systems and controls to ensure compliance with this Policy and the local legal and regulatory requirements.

#### 5.4 Employees and Intermediaries

All employees and intermediaries must comply with this Policy. Intermediaries play a vital role in establishing the profile of the customers. The ability to identify indicators of money laundering, terrorist financing and sanctions, then subsequently reporting these suspicions is crucial in fulfilling regulatory obligations of FWD and of its employees and intermediaries. Periodic anti-money laundering & terrorist financing and sanctions risk assessments are to be conducted, in particular:

- formally documented assessments segmented by products, delivery channels, types of customer and geographic location of customers
- customer due diligence procedures including identification of new customers, beneficial owners and beneficiaries
- third party due diligence procedures including background checks on third parties and employees
- customer profiling and collection of 'Know Your Customer' information
- additional due diligence in relation to high risk customers
- transaction monitoring procedures and review of alerts
- update of existing customer files in relation to 'Know Your Customer' information

#### 5.5 Human Resources

The Human Resources Department is responsible for screening employees to ensure high standards are maintained when hiring employees and on an on-going basis. The employee screening should include:

- a) Background checks with past employers; and
- b) Screening against ML/TF/Sanctions information sources.

The Human Resources Department is also responsible for maintaining and providing reports on all employees (including new hires) in respect of the completion or non-completion of the AML/CTF/Sanctions training promptly to the Compliance Department.

## 6. Three Lines of Defence

The FWD Risk Management Framework is based on the three lines of defence risk management model which provides for sound management of risks relating to AML/CTF and Sanctions. The three lines of defence set out effective guidelines in relation to functions that own and manage risks, functions that oversee risks and functions that provide independent assurance as outlined below:

### 6.1 First Line of Defence

Employees including senior management and functional heads manage the risk associated with the day-to-day activities on AML/CTF and Sanctions which include customer due diligence, identifying and reporting suspicious activities, establish an appropriate approval process for high risk circumstances, and participate in trainings.

### 6.2 Second Line of Defence

The Compliance function regularly reviews the AML/CTF and Sanctions system to ensure its effectiveness and to provide support and guidance to senior management in ensuring that the money laundering and terrorist financing risks are adequately managed. In conjunction with the legal department, the Compliance function identifies updates on laws and regulations pertaining to AML/CTF and Sanctions.

### 6.3 Third Line of Defence

Independent testing and reporting should be conducted by the Internal Audit Department. The testing should evaluate the adequacy of the overall AML/CTF and Sanctions program in addition to periodic assessment of high-priority matters and cyclical, comprehensive assessment of procedures applied.

## 7. Compliance Risk Management

FWD recognises that it is not possible to detect all potential money laundering, terrorism financing, tax and sanctions evasion activities within an organisation. FWD will have in place the following to manage the ML/TF/Sanctions risks including but not limited to:

- Law on Anti-Money Laundering and Combating the Financing of Terrorism (June 27, 2020)
- Law on Proliferation of Weapons of Mass Destruction (June 27, 2020)
- Sub-decree on Freezing of Property of Designated Terrorists and Organization (March 10, 2014)
- Directive on Customer Due Diligence Measure by the Cambodia Financial Intelligence Unit (CAFIU) (January 29, 2021)
- Prakas on Anti-Money Laundering and Combating the Financing of Terrorism relating to all Reporting Entities not regulated by the National Bank of Cambodia (December 21, 2010)
- Recommendation of the Financial Action Task Force
- Other laws and regulation requirement (if any).

### 7.1 Customer and Third-Party Due Diligence

KYC is the process of understanding and identifying the true identity of a customer. It is also the process of attaining information relating to the source of funds and source of wealth in high risk circumstances. Customer Due Diligence is the process of collecting information from the customer or third party to verify the identity. FWD assesses the AML/CTF and Sanctions risk profile of its customers and stakeholders through these processes.

This Policy defines the objectives and principles of the CDD process. FWD should define its risk based CDD and third party CDD control procedures for fulfilment of its local law and regulatory requirements as well as business needs.

FWD and its entities should conduct and complete KYC and CDD processes for its customers before the insurance policy is issued and during the course of the business relationship, particularly if any triggering events arise or any changes in the customers' circumstance which may impact his

## AML/CTF and Sanctions risk exposure.

Consistent with applicable law, CDD procedures for FWD customers should be defined to include the following:

- Identify and verify the identity of each customer before and during the course of a business relationship using up-to-date, reliable, independent source documents, data or information.
- Identify the beneficial owner of the customer and take reasonable measures to verify the identity of the beneficial owner. For entities, legal persons and arrangements this should include understanding, identifying and retaining the information in relation to the ownership and control structure of the entity, the authorized signatories, and key controllers.
- Identify and verify the identity of the beneficiary before the time of payout or when the beneficiary intends to exercise vested rights under the insurance contract.
- Obtain appropriate additional information to understand the customer's circumstances including the purpose and expected nature of the relationship.
- Assess the risk of money laundering associated with the intended (or existing) business relationship. Factors influencing the level of money laundering risk include: 1) customer risk; 2) country or geographic risk; 3) product or financial instrument risk and 4) distribution risk.
- Implement the level of due diligence commensurate with the perceived risk.

Where the customer is unable to comply or complete the KYC and CDD requirements, FWD entities should not commence business relations or perform the transaction; or terminate the business relationship; and consider making a suspicious transactions report in relation to the customer.

## 7.2 Simplified Customer Due Diligence

The standard level of due diligence may be reduced in recognised lower risk scenarios, such as:

- Customers which are publicly listed companies subject to regulatory disclosure requirements.
- Customer which are other financial institutions subject to AML/CTF and Sanctions regime consistent with FATF Recommendations.
- Life insurance policies where premium is deemed low risk as prescribed by local regulations.
- Insurance contracts for pension schemes if there is no surrender clause and the insurance contract cannot be used as collateral.

- A pension or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

The simplified measures should be consistent with the lower risk factors and should relate only to customer acceptance measures or to aspects of ongoing monitoring, such as:

- Reduce the frequency of updates on inquiries in respect to customer identification details.
- Reduce the degree of on-going monitoring and scrutinising transactions based on a reasonable monetary threshold.
- Verify the background of the customer and the identity of its ultimate beneficial owner(s) after the establishment of the business relationship.

Simplified measures are not applicable where there is suspicion of money laundering or terrorist financing or where higher risk scenarios occur, such as when there is doubt on the veracity or adequacy of customer information obtained.

### 7.3 Enhanced Customer Due Diligence

Enhanced due diligence measures should be undertaken in respect of customers deemed to be of higher risk including transactions involving higher risk countries or defined by applicable law or regulation as posing higher risk, such as Politically Exposed Persons ("PEP"), high risk and other monitored jurisdictions, high risk businesses, anonymous transactions, etc. When an application is assessed to be of higher risk, apart from discharging the duty to continuously monitor the relationship with such persons, additional risk mitigation measures and controls should be applied and these measures may include:

- A system to identify and monitor higher risk customers and transactions within business lines across the company.
- Increased levels of CDD or enhanced due diligence to strengthen the knowledge about the customer including the source of wealth and the source of funds flowing through the product.
- Escalation for approval to Senior Management or its deputy before commencement or continuation of business relationship or at trigger events.
- Increased monitoring of transactions (frequency, thresholds, volumes, etc.).
- Increased levels of ongoing controls and frequency of reviews of relationships.

Examples of High Risk Businesses might include, but not limited to:

- a. Currency exchange or money transmitters, payment service provider and shell banks
- b. Arms, defence, military and dealer/manufacturer of weapons, munitions, military related items, and atomic power
- c. Operators or dealers of virtual commodities (i.e. operating virtual commodities exchange, brokerage or transaction processing services including provision of machines/ channels that facilitate the sale and purchase of virtual commodities)
- d. Red light business/adult entertainment
- e. Registered charitable and non-profit organisations/foundations such as religious organisations

#### 7.4 Reliance on Third Parties

FWD may only rely on a third party to perform the customer due diligence measures if:

- a) the third party has demonstrated to the Company and that the Company is satisfied with the third party CDD measures are consistent with the standards of FWD; and
- b) the third party is willing and able to provide, on request and without delay, any documents or information on the customer.

BU may rely on a third party or another FWD to perform the requisite CDD measures after consulting Group Compliance.

When CDD process is conducted by intermediaries or other third parties, the following measures are to be in place:

- Immediately obtain from the intermediary the necessary CDD information and documentation.
- Ensure that the intermediary is regulated and supervised with adequate measures to comply with all CDD requirements and record keeping obligations.
- Intermediaries are responsible for the validity of the CDD information and documentation obtained.

Where such reliance is being carried out, the ultimate responsibility for CDD measures remains with FWD. Any CDD exercise conducted by an intermediary should be subject to the same standard adopted by FWD.



## 7.5 Due Diligence on Third Parties

Due diligence on Third Parties (also known as background check) should be conducted and completed for its agents, as well as employees, before entering into agreement/contract with them, as well as before renewing the agreement/contract. At minimum, the following information and controls should be obtained and implemented during the third-party background check:

- Basic personal/entity information and contact details of the contracted party.
- Understand the company's AML/CTF and Sanctions compliance status.
- Name screen the company and principal shareholders and officers.

A risk based approach is adopted to conduct the AML/CTF and Sanctions due diligence when procuring goods and services from third parties. See the Group Procurement Policy for details.

## 7.6 On-going monitoring of customers

On-going monitoring is crucial as a customer profile may change over time. A key part of ongoing monitoring includes maintaining relevant and up-to-date CDD data, documents and information particularly for high risk customers, so that the Company can identify changes to the customer's risk profile. For non-high risk customers, the Company should obtain updated CDD information upon occurrence of a triggering event. On a regular basis or upon a trigger event, customer profile is to be updated and their transactions and activities are to be revised to ensure that they are in accordance with information provided.

## 8 Monitoring of Customers and Transactions

The purpose of monitoring is to identify customers whose activities appear to be unusual and which require further analysis to determine if there are grounds for further concern. The degree of monitoring will be based on the perceived risks associated with the customer, products or services being used by the customer and the location of the customer and the transactions. Monitoring could be based on monetary or other thresholds to identify transactions according to size or type to be reviewed. The results of the monitoring should be recorded. At a minimum, FWD should ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking periodic reviews of existing records, particularly for higher-risk categories of customers.

## 9 Recognising and Reporting Suspicious Activities

### 9.1 Reporting Suspicious Activities

Where an employee has knowledge or suspicion of money laundering, terrorist financing or sanctions activity, it must be reported according to procedures established by the local offices on reporting of suspicious activities. Intermediaries also have responsibility in bringing potential suspicious behavior to FWD's attention and in responding to FWD's requests for information in the course of reviews on clients and clients' activities. Key principles in establishing the reporting procedures may include:

- Employees should be made aware that they must report any knowledge or suspicion of money laundering or terrorist financing activities to its MLRO;
- The MLRO will determine whether the report gives rise to plausible suspicion, requires investigation into the suspicion, and finally whether reporting to the local authorities is required;
- Proper records, including the analysis on actions taken or not, must be kept for all suspicious activity reporting by the MLRO;
- All information pertaining to suspicious activity reporting are treated with complete confidentiality and should remain with MLRO;
- Tipping off offences are very serious and therefore any reports provided to the MLRO should be confidential unless it is requested by law enforcement agencies or an internal FWD employee who has a need to know. Sharing of any information related to a suspicious transaction report to unrelated 3<sup>rd</sup> parties is strictly prohibited.

### 9.2 Recognising Suspicious Activities

Suspicious may be aroused as a result of one or a combination of the followings:

- a. conceal identity of customer, beneficial owner or ownership of funds;
- b. incomplete application details and lack of willingness to provide evidence to required information;
- c. customer's address is outside the local service area;
- d. investment taken against advice or not appropriate to customer's true needs;
- e. third party transactions (payments in or out);
- f. cash payments or withdrawal requests;

- g. multiple sources of payments;
- h. cross jurisdiction funding for payments;
- i. payment of premium from early surrender of another investment in unusual circumstances;
- j. unnecessarily complex and/or unusual transactions or intentions, or patterns of transactions;
- k. immediate interest in surrender penalties or loans and a lack of interest in benefits during application stage;
- l. early surrender of contract or termination of contract during cooling-off period;
- m. receipt of unexplained telegraphic transfers and/or requests to return telegraphic transfers;
- n. request for no correspondence to go to policyholder;
- o. complex ownership structures involving layers of companies and/or trusts;
- p. suspicious behavior of either customer or introducer.

The existence of any one or more of the above circumstances does not necessarily indicate an act of money laundering. Where any of the above circumstances gives legitimate cause for concern, a report must be made according to the suspicious activities reporting procedures.

## 10 Record Keeping

All customer identification records, transaction and account records, including risk assessment results at onboarding and triggering events, and business correspondence must be kept and maintained so that they can be made available to the relevant authorities in a timely fashion. The retention period is to be dictated as per local regulatory requirements of each respective country.

## 11 Training and Awareness

All employees will receive a minimum level of general information on AML/CTF and Sanctions laws, regulations and internal policies through training sessions. New joiners should complete the training as soon as reasonably practicable after commencement of employment. Subsequent refresher trainings are to be conducted on an annual basis. Training should be tailored at an appropriate level of detail according to responsibilities of the individual employee.

Intermediaries are to receive equivalent training as stipulated in their respective contract of engagement. Records of the trainings, including completion record and training materials, must be

kept in line with local regulatory requirements.

## 12 High-risk and Other Monitored Jurisdictions

Financial Action Task Force (“FATF”), among other organization, identifies the jurisdictions with weak measures to combat money laundering and terrorist financing. A list of high risk countries is being maintained by the MLRO.

## 13 Sanctions

### 13.1 Sanctions and Its Associated Risks

‘Sanctions’, in general, refer to economic sanctions imposed by authorities in jurisdictions in which FWD operates. These sanctions can target individuals, entities, government (‘Sanctioned Persons’) or entire jurisdictions (‘Sanctioned Jurisdictions’), or certain types of activities (‘Sanctionable activities’).

Sanctions may be comprehensive or targeted and may involve arms embargoes, trade restrictions or embargoes, freezing of assets, travel bans, etc. Sanctions are usually issued to accomplish foreign policy and national security objectives, or to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and stop the proliferation of weapons of mass destruction.

Sanctions risks, in general, refer to the risks of potential or actual violations of sanctions. FWD may be exposed to sanctions risks arising from (a) counterparty or (b) customers, and (c) their ultimate beneficial owner, shareholder, management or related company.

FWD is committed to complying with sanctions restrictions against specified individuals, countries and businesses issued by international governing bodies as well as the sanctions regulations in the jurisdictions in which FWD operates. The Company shall ensure that any customers, their relatives or close associates, connected parties, business counterparties or any third parties that are subject to international sanctions or embargoes are escalated to Group Compliance for assessment. A breach of sanctions requirements carries heavy penalties for FWD and our employees.

The Company shall establish and maintain effective and appropriate Policies, Procedures, systems and controls for ensuring that its business is conducted in compliance with legal and regulatory requirements relating to sanctions in the jurisdiction in which it operates. In addition to the locally issued sanctions requirements (which may differ between jurisdictions), the Company should

consider the sanctions issued by the following governing bodies in formulating its Policies and Procedures:

- United Nations Security Council Consolidated Sanctions List (“UN”);
- European Union’s (“EU”) consolidated list of persons, groups and entities;
- US Department of Treasury, Office of Foreign Assets Controls (“OFAC”);
- UK HM Treasury (“HMT”), Office of Financial Sanctions Implementation consolidated list of targets.

Request for exemptions from this Policy shall be made in accordance with the Group’s Enterprise Risk Management Policy. Group Compliance will consider the exemption requests and discuss with Group Risk and Group Legal, as appropriate.

Any sanctioned customers or where their relatives or close associates, connected parties or business counterparties, third parties identified with sanctions related adverse news relating to Sanctioned Persons, Sanctioned Jurisdictions and/or sanctionable activities, either at the on-boarding stage, or during the subsequent screening, need to be escalated to Group Compliance for the assessment of implications, and the determination of any actions such as reporting to the related governing bodies, suspension of premium or benefit payments, or termination of the business relationship, as appropriate.

### 13.2 Proliferation Financing

Proliferation Financing (“PF”) risks and sanctions risks are closely intertwined as the Democratic People’s Republic of Korea (“DPRK”) and Iran are the primary countries of proliferation concern.

PF is defined as providing funds or financial services to manufacture, export, transfer or use nuclear, chemical or biological weapons and related materials and their means of delivery. It involves in particular the financing of trade in proliferation sensitive goods but could also include other financial support to individuals or entities engaged in proliferation activities. The UN Security Council has used list based targeted financial sanctions and activity based financial prohibitions and economic/sectoral sanctions to augment the tools to combat PF.

FWD is committed to play its role as a gatekeeper to safeguard the Company from being used as a tool for PF and sanctions evasion. In this regard, FWD has in place controls and measures to detect and prevent PF activities and transactions. This includes being vigilant regarding the risks of establishing or maintaining business relationships with customers that are from or associated with

countries of proliferation concern such as Iran and DPRK.

### 13.3 Insulation of US Persons and European Union Persons

OFAC sanctions prohibits the involvement of US Persons in transactions involving OFAC sanctioned countries or territories or OFAC sanctioned targets (e.g. SDNs) unless authorised under an applicable license. Accordingly, all officers and employees including contractors or agents engaged by the Company, who are US Persons or operating in the US must not participate in or otherwise support or facilitate such transactions.

The above provision correspondingly applies to officers and employees including contractors or agents by the Company, who are European Union Persons in respect of sanctions issued by the EU unless permitted under the relevant EU sanctions. 'Officers' refers to directors of the board of directors and the management committee of the Company.

## 14 Screening

It is imperative that terrorist suspects and designated parties, as per the obligations set out in the relevant Sanctions laws and regulations, can be identified when dealing with customers, third parties and employees.

Screening procedures must be in place utilising a data base specialised in this type of activity.

Any potential alert identified during a screening exercise must be reviewed, resolved and reported in accordance with the local suspicious activities reporting procedures. Any identified customers subject to international sanctions needs to be escalated to Group Compliance for decisions.

## 15 Transparency

FWD employees may not knowingly change, alter, delete, exclude or otherwise modify transaction or payment details or information with the intent to disguise or conceal the existence of a party, jurisdiction or other element that might involve sanctions, money laundering or terrorist financing related concerns.

## 16 Reporting

The Company shall submit an Enterprise Wide Risk Assessment to Group Compliance once every two years detailing the status of its AML/CTF and Sanctions Program, which includes the following:

- A summary of key AML/CTF and Sanctions requirements and any material changes in such requirements from the previous submission, if any.
- A summary of the results of the annual AML/CTF and Sanctions risk assessment, including key findings and action plans arising therefrom.
- A description of any regulatory examinations or audits (external or internal) undertaken, including key findings.

All issues that may have a material impact on the Group, including regulatory sanctions, adverse public media, or any high risk cases (e.g., high risk customers and suspicious transactions subject to the local regulations on non-tipping off and confidentiality), must be escalated immediately to Group Compliance.

## 17 Definitions

“Employee” - Refers to anyone who is permanently or temporarily employed by the Company or on secondment / as a trainee with the Company, which includes all Board members, Management, and other staff of the Company.

“Money Laundering” - The act of making any funds that are the proceeds obtained from an unlawful activity appear legitimate by disguising their source/origins, nature, location, ownership, or control.

“Politically Exposed Person (PEP)” - Is an individual or legal entity who is entrusted with a prominent public function in a place within (i.e. Domestic) or outside (i.e. Foreign) the place of the business of the Company, or by an international organization, their immediate family or persons known to be close associates of such persons.

International organizations are entities established by formal political agreements between their member countries and recognized by law in their member countries.

“Reason to know” - with respect to a fact, means that:

- a person has knowledge of the fact; or
- from all the facts and circumstances known to the person without investigation, the person

should be aware that the fact exists.

“Terrorist Financing” - The provision or collection, by any means, directly or indirectly, of any property with the intention that the property be used, or knowing that the property will be used, to facilitate or carry out terrorist acts regardless of whether the property involved in the transaction were proceeds of unlawful activity or were derived from lawful activity.

“Third Parties” - Refers to any supplier, vendor, consultant, (sub) contractor or provider, whether an individual or an entity, providing goods and / or services to FWD.

“Tipping Off” - Refers to a person making disclosure to any other person any information which is likely to prejudice an investigation that may be conducted following such disclosure.

“Close Associate” - Means a natural person who is closely connected to the subject being considered (which could be a Politically Exposed Person, a Special Interest Person, a Sanctioned Person, or a customer) either socially or professionally.

“Connected Party” means:

- a) a legal person, means any director or any natural person having executive authority in the legal person;
- b) a legal person that is a partnership, means any partner or manager, and
- c) a legal arrangement, means any natural person having executive authority in the legal arrangement.

“Customer” - Means a person (whether a natural person, business or other entity, legal person or legal arrangement) with whom the company establishes or intends to establish a business relationship.

“EU Person” means:

- a) Any person who is a national of an EU Member State, even if based outside the EU;
- b) Any legal person, entity or body wherever incorporated/constituted, in respect of any business done in whole or in part within the EU; and
- c) Any person within the EU, irrespective of their nationality.

“United States Person” or “US Person” means:



- a) All US citizens and permanent resident aliens (e.g. green card holders) regardless of where they are located;
- b) All individuals and entities located within the United States (including financial institutions);
- c) All US incorporated entities and their foreign branches; and
- d) In the cases of certain program, such as Cuba and Iran, foreign subsidiaries owned or controlled by US companies also must comply.

“Ultimate Beneficial Owner” - Refers to the natural person who ultimately owns 25% or more of the customer or controls a customer, and/or the natural person on whose behalf a transaction is being conducted or business relations are established and includes the person who exercises ultimate effective control over a legal person or arrangement, or over the customer’s policy.

“Triggering Event” - Refers to any of the events that should trigger a review of a customer.

## 18 Sources of Further Information

### 18.1 Financial Action Task Force (FATF)

The Financial Action Task Force (“FATF”) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. <http://www.fatf-gafi.org/>

### 18.2 International Association of Insurance Supervisors (IAIS)

The International Association of Insurance Supervisors represents insurance regulators and supervisors of over 130 countries whose objective is to promote efficient, fair, safe and stable insurance markets for the benefit and protection of policyholders; and to contribute to global financial stability. IAIS has published principles, standards and guidance papers in relation to anti-money laundering and combating financing of terrorism. <http://www.iaisweb.org/>

### 18.3 Transparency International

Transparency International is a global non-profit organization created with a mission to combat corruption and to prevent criminal activities arising from corruption. It publishes the Corruption Perception Index annually which ranks countries and territories based on how corrupt their public

sector is perceived. [www.transparency.org/](http://www.transparency.org/)

C2 - Internal



## FWD Anti-Bribery and Corruption Policy (ABCP)

Document ID	KH-COM-PO-0010	Document type	Policy
Issued by / Owner	Chief Corporate Governance Officer	Approved by	Board of Directors
Target audience	All managements, directors, employees, contingent workers and contractors at all levels		
Document status	In-effect	Date Last Approved	16 August 2023

### Document approval history

Version	Date approved	Description
1.0	3 August 2022	First Version
1.1	16 August 2023	Annual Refresher of the Policy

## Contents

1.	Policy Statement .....	3
2.	Anti-Bribery & Corruption (ABC) Compliance Programme .....	3
3.	Policy Objective .....	3
4.	Scope of Application .....	4
5.	Policy Ownership and Review Information .....	4
6.	Policy Requirements.....	4
	ABC 1 Top Level Commitment .....	4
	ABC 2 Identification and Assessment of Bribery and Corruption Risk .....	5
	ABC 3 Facilitation Payment .....	6
	ABC 4 Gift and Hospitality (G&H).....	6
	ABC 5 Sales incentive program and training to sales intermediary.....	8
	ABC 6 Due Diligence (DD) .....	8
	ABC 7 Political Donations, Charitable Donations, Sponsorship and Community Investment Activities.....	10
	ABC 8 Reporting and Escalation .....	11
	ABC 9 Training and Awareness.....	12
	ABC 10 Monitoring and Assurance .....	13
	ABC 11 Record Keeping.....	13
7.	Definitions .....	13
8.	Dispensation .....	14
	Appendix 1 Roles and Responsibilities .....	15
	Appendix 2 Red Flags and Risk Events for Bribery & Corruption .....	17

## Policy Statement

FWD Life Insurance (Cambodia) PLC. (the “Company”) is committed to conducting business in accordance with the highest ethical standards and has zero tolerance towards bribery and corruption. The Company prohibits all forms of bribery and corruption. The Company will not seek to influence others, either directly or indirectly, by offering, paying or receiving bribe or kickback, or by any other means that is considered unethical, illegal or harmful to our reputation for honesty and integrity.

All employees and representatives of the Company have the responsibilities to:

- Comply and uphold the Company’s commitment on anti-bribery and corruption in their undertaking of performance of their services for, and on behalf of the Company.
- Report any concerns on bribery and corruption through relevant channels.

### 1. Anti-Bribery & Corruption (ABC) Compliance Programme

The Company has in place a compliance programme to manage bribery and corruption risks.

The programme comprises of:

- a) **Written policies and standards:** The Company Policy on Anti-Bribery and Corruption sets out the Company’s commitment, key principles and standards on anti-bribery and corruption. It is supplemented by other various policies and standards which address specific areas of bribery and corruption risk.
- b) **Risk identification and assessment:** The Company leverages on its self-assessment process where Business Units would identify and assess key risks including bribery and corruption risks. In addition, the Company will have to conduct a Group-wide Risk Assessment based on the Company’s methodology.
- c) **Training and Communication:** the Company requires all employees to undergo periodic ABC training to enhance the awareness and understanding of the Company’s commitment on ABC. In addition, the Company communicates its stance on bribery and corruption to third party service providers via provision of ABC clauses in outsourcing agreements.
- d) **Reporting:** the Company leverages on its whistle-blowing program that provides a channel for employees and external parties to raise concerns relating to bribery, corruption, suspected fraud, misconduct or any other irregularities without fear of reprisal.

### 2. Policy Objective

The purpose of this Anti-Bribery and Corruption (ABC) Policy is to establish the framework to conform to the Hong Kong Prevention of Bribery Ordinance (POBO) and the anti-bribery and corruption laws in

all jurisdictions in which the Group Office (Group) operates and to ensure FWD's business is conducted in a honest and ethical manner.

In addition to the standards established in this Policy, it is the responsibility of executive management in all jurisdictions where the Group operates to ensure full compliance with all applicable regulatory and statutory requirements. The Company should discuss with Group Compliance any perceived conflict between Group Policy and local regulatory and statutory requirements.

### 3. Scope of Application

This Policy applies to all managements, directors and employees of the Company and is mandatory. Requirements of this Policy must be read and complied with in conjunction with the Anti-Bribery and Corruption Standards, Anti-Money Laundering (AML) Policy, Code of Ethics, Conflict of Interest Policy, Whistleblower Policy and Delegated Authorities Table.

### 4. Policy Ownership and Review Information

This Policy is owned by the Chief Corporate Governance Officer (CCGO). The Compliance maintains the Policy on the CLCO's behalf, taking advice from the Corporate Governance Committee (CGC), and internal and external legal counsel. This Policy is reviewed and recommended for approval by the Board. Compliance is required to review the scope and wording of the Policy at least once every two years to determine whether changes are required.

### 5. Policy Requirements

#### ABC 1 Top Level Commitment

The Board and Senior Management must foster a culture of integrity where bribery and corruption are unacceptable and commit to prevent bribery by persons associated with the Company. Senior Management must put in place a clear ABC framework and provide regular communication to employees on ABC.

**ABC 1.1** Employees occupying leadership roles must act as a role model and build a transparent, safe and trustful culture within their teams and to ensure that there are sufficient processes and resources to undertake the required roles and responsibilities for the effective operation of the ABC Programme.

**ABC 1.2** The Company's CEO is required to appoint a suitable person as the Anti-Bribery and Corruption Officer (ABCO) to lead the ABC function with a reporting line to the appropriate senior management in order to oversee the application of the Company Policy in the Company. ABC compliance responsibilities should be documented clearly in the official job description for all ABC roles and organisation charts outlining the ABC function within the company structure.

## ABC 2 Identification and Assessment of Bribery and Corruption Risk

An enterprise-wide risk assessment on bribery and corruption risk must be performed by the Company once every two years, or more frequently where the risks of the relevant business warrant it. The risk assessment result must be properly reviewed, approved and documented by the Company.

**ABC 2.1** The Company must conduct a risk assessment to ensure that inherent risks to the business relating to potential bribery and corruption are identified, controls are implemented to mitigate these risks, residual risks are assessed and accepted by the senior management. The ABC risk assessment template provided by Group Compliance must be used to document the risk assessment

The process followed to conduct the risk assessment, the results of the risk assessment and the controls that have been put in place must be documented by the management teams with the support of the ABCO. The functions that are expected to be involved in the assessment include, but are not limited to Compliance, Finance, HR, Marketing, Distribution, Procurement, Government Relations, Legal and Operations. The Company must be able to demonstrate:

- The assessment of bribery and corruption risk;
- The implementation of appropriate systems and procedures;
- The monitoring, review and enhancement (if necessary) of the effectiveness of its control;
- The reporting process to senior management on the operation of its control processes;
- The application of risk-based assessment and controls;
- The risk mitigation strategy has been approved by senior management and relevant board committee; and
- The risk assessment and strategy are kept under review and updated when a new risk presents itself.

**ABC 2.2** the Company must continue to review and monitor the risk environment to ensure that the risk assessment result is relevant and up-to-date, any new risk exposures are identified and documented, and new controls are implemented if appropriate. Controls must be tested on a periodic basis as deemed appropriate by the Company ABCO to ensure they are working effectively.

**ABC 2.3** The completed risk assessment must be reviewed and approved by the ABCO and an executive summary of the assessment must be provided to the CGC as appropriate for noting. The completed risk assessment must be submitted to Group Compliance for review in accordance to the timeline provided by Group Compliance.

**ABC 2.4** When there is any new business initiative such as launch of new product or new distribution channel, the ABCO must take an active role to ensure bribery and corruption risks are considered during the approval process for these new business initiatives.

### ABC 3 Facilitation Payment

Facilitation payments are any payment made to facilitate or expedite the performance of a routine transaction or service to which the person or company making the payment is legally entitled to receive. It does not include those payment comprised in a lawful and published tariff available to all. ABCP prohibits any facilitation payment and all such instances must be reported to Compliance promptly. Any legitimate cost for obtaining services should be clearly documented and accurately recorded in the Company's accounting records.

**ABC 3.1** Facilitation payments may be unavoidable in exceptional circumstances due to a threat to or impact on the health and safety of an employee. In any such duress situation, the safety of employees takes priority. The Company must establish procedures for all employees to ensure any facilitation payments or other such payments made under duress or threats to the safety of persons are immediately reported to their line manager, ABCO and Compliance and are accurately documented and recorded in the Company's accounting records.

### ABC 4 Gift and Hospitality (G&H)

G&H must not be used to influence, or appear to influence, external parties or encourage favoritism for discharging of services or improper actions of another party. The Company must establish clear processes and requirements to maintain a G&H register, including guidelines on pre-approval, value thresholds for recording entries, reporting and consequence for non-compliance.

**ABC 4.1** Employees must not request, accept, offer or provide G&H designed to induce, support or reward improper conduct including in connection with any business or anticipated further business involving the Group. This requirement extends to the provision or acceptance of G&H through any third-parties or to or by members of the family of an employee of an actual or potential customer.

The following G&H are prohibited and considered a breach of this Policy:

- Gift of cash and cash equivalent (such as, but not limited to, gift cards or vouchers<sup>1</sup>) to/from any government officials. Gift of cash and cash equivalent to/from other external third parties should be avoided unless relevant approval is obtained in advance in accordance to the ABC Standards;
- Gift of luxury products (e.g. designer handbags) with value more than USD 1,500 per item;
- G&H that are indecent, inappropriate or could damage the Group reputation for integrity;

---

<sup>1</sup> Gift card, voucher etc which cannot be redeemed for cash is permissible.



- G&H received from or offered to any third party which may be perceived to give rise to a conflict of interest; and
- G&H that breach any local law and regulation or that the recipient is not permitted to receive by their employer.

**ABC 4.2** Employees must obtain approval before offering or accepting G&H to/from any external third party in line with the thresholds and approval limits determined in this policy, the ABC Standards and other policy and procedure. A G&H register must be established to record all G&Hs offered, accepted or rejected to and from government officials and all other G&H offered/received requiring approval. This register should demonstrate the consideration and mitigation of any potential ABC risks that may be present for each activity and the rationale of offering/receiving the G&H.

**ABC 4.3** All G&H offered or received must be reasonable in cost, quantity and frequency and permitted under local law and regulation. In addition, G&Hs offered by the Company must be given openly and transparently and properly recorded in the Company's accounting records. Ceremonial gifts that are customary during festivals or any other local celebratory traditions are not prohibited but must be proportionate, properly recorded and provided only to reflect esteem or gratitude.

**ABC 4.4** All G&H provided to or received from government officials must be properly approved, monitored, recorded in the G&H register and included within quarterly ABC Management Information (MI) report. The Company prohibits the offer, promise, or provision of money (cash or other forms of transferable value), gifts, entertainment, hospitality, travel, or anything else of value to any government officials, for the purpose of influencing such officials in order to obtain or retain business or a business advantage, or otherwise in relation to decisions that may be seen as beneficial to the Company's business interests.

**ABC 4.5** Training trips (e.g. conferences, seminars, etc.) provided to third parties (other than sales intermediaries as detailed in ABC 5), particularly those provided to government officials, must be subject to pre-approval and appropriate due diligence in order to ensure there is a legitimate rationale and that it is not made to obtain any improper advantage. The Company must limit overseas training to occasions where there is a clear and justifiable business rationale for both those invited and for the chosen location. All training trips provided must be subject to the same standard applied under the Company Travel Policy for the Company's employees and must be recorded accurately in the books and records.

**ABC 4.6** All G&Hs provided to sales intermediaries (except those provided in a sales incentive program/activity covered in ABC 5) must be subject to the same approval and recording process of G&H provided to other external parties. Normal business meals and gifts provided to tied insurance agents who are directly contracted with the Company and sell Company's products exclusively can be exempted from the G&H approval process. However, appropriate record and receipt of such meals and gifts should still be retained by the Company.

**ABC 4.7** The Company must not make requests to current or potential vendors asking for sponsorship or contribution to the cost of staff events such as cash or prizes for lucky draw prizes. Such request could be perceived as inducements to maintain current business relationship and pose a bribery and corruption risk.

## **ABC 5 Sales incentive program and training to sales intermediary**

The Company must ensure any sales incentive program and training provided to sales intermediary are undertaken and approved in line with agreed and documented processes. All such activities must be assessed for bribery and corruption risks. Advice should also be obtained from ABCO when there is any concern before any commitments are made. All such activities must be properly documented and accurately recorded in the Company books and records.

**ABC 5.1** Sales incentive program or activity provided to sales intermediary, e.g. incentive trips, must be used to encourage voluntary and ethical behaviours for generating legitimate business to the Company. All sales incentive programs and activities must be designed for commercial reasons and be supported by proper business rationales. It should be properly budgeted and be pre-approved in line with the approval limit determined in the Delegated Authorities. All sales incentive programs and activities must be reviewed and approved by Group Distribution (for those program or activities required to be escalated to Group as per the Group Delegated Authorities). As part of the approval process, Distribution must ensure bribery and corruption risks are properly assessed and satisfy that all such programs /activities are not leveraged for channeling bribes. Any unbudgeted or unplanned (“ad hoc”) sales incentive to a sales intermediary must be approved by the CEO and the Chiefs of Distribution in addition to any approval requirement described in the Delegated Authorities. Advice should also be obtained from ABCO when there are any concerns prior to making any commitments.

**ABC 5.2** All training (e.g. conferences, seminars, etc.) provided to a sales intermediary must be supported by a genuine business purpose and have a clear business agenda. It should be appropriately budgeted and approved in line with the Delegated Authorities. All trainings must be supported by appropriate records and recorded in the accounting records accurately.

## **ABC 6 Due Diligence (DD)**

Appropriate DD must be undertaken by the Company prior to entering any relationship with any third party and prior to making any offer to any potential employee, contingent worker, or intern. Regular refresher DD must also be undertaken by the Company on all third parties and existing employees, contingent workers and interns.

**ABC 6.1** To achieve effective procedures to counter bribery and corruption, the Company should have a clear understanding of its third party population. Third parties for purposes of this Policy include but are not limited to:

- Joint Venture and M&A intermediaries/partners;
- Bancassurance and other Distribution partners;
- Sales Intermediaries e.g. Insurance Brokers and Agents;
- Employees, Contingent Workers and Interns;
- Sponsorship partners and Community Investment partners, e.g., charities or NGOs;
- Suppliers of goods and services; and
- Customers<sup>2</sup>

The Company should rate their third parties based on the risk they represent to the business at onboarding. Relevant risk factors such as geographic location, nature of service to be performed, connections with government officials etc. should be considered in the risk assessment. The risk rating should be used to determine the appropriate level of DD to be carried out on the third party relationship.

**ABC 6.2** The Company should undertake appropriate and proportionate risk-based DD before entering any engagement with third parties and conduct refresher DD on a regular basis in order to ensure that the third party relationship may be maintained. Refresher DD must be performed at least annually for third parties that are rated high risk and regularly for third parties rated medium or low risks. All DD activities carried out and any decision made should be properly documented and retained.

**ABC 6.3** Third parties engaged to represent the Company's interest must comply with FWD Code of Ethics and Business Conduct. Contract owners are responsible for ensuring that the Company's expectations on ABC are communicated to and followed by third parties, and that such third parties are, where required, provided with the necessary awareness materials. Further, contract owners must ensure that appropriate contractual protections and safeguards are in place where necessary. It is important to ensure that such provisions are used in agreements where the third party has affirmatively agreed to such provisions and not just included passively (i.e. there should be some acknowledgement or engagement to ensure that third-parties are aware of the Policy and position of the Company with regards to ABC either via messaging, on-boarding or provision of awareness materials). Please refer to the ABC Standards for the details of the ABC contract clause.

**ABC 6.4** All employees, contingent workers and interns performing services for the Company are capable of committing bribery on the Company's behalf. The Company should therefore establish and maintain a robust recruitment and DD process that can support the legitimate recruitment of persons and mitigate the risk of hiring persons that may be seen as an act of bribery or may act inappropriately

---

<sup>2</sup> Refer to AML Policy for DD on customers

in the course of their employment. Appropriate DD records should be maintained to support the completion of the DD check and document the rationale of the decisions made.

## ABC 7 Political Donations, Charitable Donations, Sponsorship and Community Investment Activities

Political donations made on behalf of the Company are prohibited. Employee may choose to make payments from their own money, but not with an intention to influence a third party for the benefit of FWD or in any way that might give the impression that such influence was intended or connected with FWD.

The Company must ensure any charitable donation, community investment and sponsorship activity are undertaken and approved in line with agreed and documented processes. All such activities must be assessed for bribery and corruption risks and be subject to appropriate DD.

**ABCS 7.1** Sponsorship, for the purpose of this Policy, refers to a commercial agreement to support an entity or event which provides marketing, branding or promotional rights to the sponsoring organisation. Sponsorship and charitable donation can be anything of value (including money, gift in kind, access to or use of, or association with the group's brand or image, employee time or other resources) offered or given to an entity or event outside of the Group.

All sponsorships and charitable donations offered or provided must:

- Undertake appropriate due diligence on the ultimate beneficiary before any commitment is made. This is to ascertain whether there is any connection between the beneficiary and any business transaction with which the organization is involved, or is likely to be involved, and to confirm there are no conflicts of interest or apparent risks of unethical or corrupt behaviour. The level of due diligence required must be proportionate to the value given.
- Be properly documented and recorded with supporting rationale for the decision made and sufficient records e.g. agreement, receipt etc. for the contribution provided.
- Be properly approved in accordance to the thresholds and approval limit determined by the Company. The manager approving the expenditure must be satisfied that the sponsorship or charitable donation is appropriate, is not corrupt, and could not reasonably be perceived as being corrupt.
- Be legitimate and never made in exchange for obtaining an inappropriate advantage or could be reasonably perceived as corrupt. If it could be intended to induce someone to act improperly, it must not be offered or accepted.
- Not influence or appear to influence the independence of the giver or receiver, and in the case of a charitable donation, should be given directly to qualifying organisations defined in the Group Community Care Policy, in good faith and be reasonable in value and frequency.

- Be compliant with the applicable laws and regulations of the territory and the policies and procedures of the recipient entity.

## ABC 8 Reporting and Escalation

A process must be established by the Company for employees to report breaches or concerns relating to bribery and corruption. Regulatory or policy breaches, regular management information and any other significant ABC issues must be reported promptly to the Chief Corporate Governance Officer.

**ABC 8.1** The following issues must be promptly reported to the Chief Corporate Governance Officer

- Any breach of this policy;
- Any suspected breach of ABC law and regulation that may be significant;
- Any suspected insignificant breach of ABC law and regulation which is repeated in such a way as to suggest the breakdown of controls should be regarded as significant;
- Any other matter which ABCO consider to be significant; or

Any matters that may:

- Result from or constitute a fraudulent or criminal act involving dishonesty;
- Give risk to disciplinary action by the relevant authorities or regulators (other than minor matters of an administrative nature);
- Generate adverse publicity such as to damage the Company's reputation;
- Give rise to the risk of a significant fine and/or cost levies by a court of law, relevant authorities or regulators;
- Involve the risk of a significant monetary loss to the Company (other than a fine or regulatory costs);
- Result in the disciplining or dismissal (or forced resignation) of an employee; or
- Prompt an enhancement or addition to group policy, designed to prevent a repetition.

**ABC 8.2** The Company should report sufficient information to the local Board or any other relevant local committee on a regular basis to ensure proper visibility and management of the bribery and corruption risks. The Company should submit regular ABC report including quarterly ABC MI report, Compliance monthly report etc. to Group Compliance timely.

**ABC 8.3** Where information is requested by Compliance, either as part of an internal or external review, investigation or due to a regulatory request from the Company's lead regulator, the Company must deal with such requests promptly. All employees have a duty to comply with such requests and must not interfere or obstruct the process (including failing to keep matters confidential when instructed to do so).

**ABC 8.4** All employees are required to assist in tackling bribery and corruption. If any employee is aware of or suspects that bribery may be taking place within the group, they must report their suspicions to their line manager, ABCO, Compliance or via the whistleblowing process.

## **ABC 9 Training and Awareness**

The Company must ensure that its bribery prevention policies and procedures are embedded and understood throughout the company through training and communication. The Company must ensure all employees undertake mandatory ABC training in a timely manner and all training materials and completion record must be properly maintained.

**ABC 9.1** ABC induction training must be provided to all new relevant staff within 1 month after joining. ABC refresher training must also be provided to all existing relevant staff at least annually. Relevant staff includes:

- Permanent staff;
- Active tied agents (as per the Company definition); and
- Contingent workers, temporary staff and interns<sup>3</sup>

**ABC 9.2** Level of training must be proportionate to roles and responsibilities with advanced training for employees undertaking roles categorized as higher risk, and for senior management. The Company should identify different training requirements across their relevant staffs and deliver a training programme to ensure all relevant staff receive necessary support and training, upon joining the company or taking on a new role in a different category. A declaration concerning compliance with this Policy must be made by all relevant staff as part of the standard induction and refresher training.

**ABC 9.3** All ABC training materials should be reviewed at least annually and signed off by the ABCO and Compliance (for training materials developed by Compliance) to ensure contents are up-to-date and adequate.

---

<sup>3</sup> This includes contingent workers, consultants, temporary staff or interns who are either directly under FWD's payroll or assigned to work at FWD and salary paid via a service provider or recruitment agency. Contingent workers contracting through an organization where there is an expectation that they will have received training through their own organization and temporary staff who work on a very short term, i.e. less than four weeks, can be excluded from the training.

**ABC 9.4** The Company should track the completion of the training and maintain proper records. Appropriate actions such as escalating the matters to the risk or audit committee should be taken where mandatory training has not been completed unless there are mitigating factors.

## **ABC 10 Monitoring and Assurance**

The Company must have sufficient means in place to monitor and review the effectiveness and appropriateness of its ABC systems and controls to ensure compliance with this Policy and the local legal and regulatory requirements.

**ABC 10.1** The Company must develop an annual risk-based compliance monitoring and assurance plan by taking into consideration the annual ABC risk assessment result and the quarterly ABC MI reports. The compliance monitoring and assurance plan should be shared with Group Compliance once available for endorsement. Key ABC controls should be reviewed and tested at least annually (or more frequently where the risk of the business warrant it) by either the compliance monitoring team or internal audit to ensure they remain adequate and are performing effectively. Evidence to support completion of the review and any remedial actions should be maintained. The review and assurance process undertaken by the Company should be carried out in addition to any assurance review carried out at group level, unless agreed by the Group Chief Compliance Officer that unnecessary duplication would result.

## **ABC 11 Record Keeping**

The Company must establish a robust procedure on documentation and record retention to ensure proper records, documents and information are retained for audit trail purpose. Records of information shall be retained throughout the continuation of the business relationship and for 5 years (or longer as required by local law and regulation) after the business relationship with the relevant third party has ended.

## **6. Definitions**

For the purposes of this policy,

“Books and Records”: Public companies must make and keep books, records and accounts that, in reasonable detail, accurately and fairly reflect its transactions and dispositions of assets regardless of materiality..

“Bribery”: refers to the offering, accepting or giving of financial or other advantage that is intended to induce or reward improper performance or non-performance of a business or a public function. This includes both the offering, promising or giving a bribe as well as requesting, agreeing to receive or



accepting a bribe. It also includes asking another person to offer or accept a bribe on the employee or the Group's behalf.

“Charitable Donation”: refers to a gift made by an individual or a company to a qualifying organisation defined in the Group Community Care Policy.

“Corruption”: refers to the abuse of entrusted power or public office for a personal gain.

“Gift”: refers to an object or item of any value given to a persons or persons, apart from hospitality as defined below, in recognition of an event, or special occasions but not routinely given without a clear purpose.

“Government Official”: includes top management such as Board of Directors, Executive Committee members, persons with sufficient authority etc on behalf of any:

- Government, or department, ministry, agency, authority, or branch of government;
- State-Owned or State-Controlled Enterprise;
- Political party or office; or
- Public international organisation.

“Hospitality”: refers to provision of meals, entertainment, travel and accommodation.

“Sponsorship”: refers to a commercial agreement to support an entity or event which provides marketing, branding or promotional rights to the sponsoring organisation.

“Representative”: Third parties who are retained to perform services or conduct business for and on behalf of the Company or those conducting business together with the company (including, but not limited to, agents, intermediaries, introducers, brokers, contractors, suppliers, consultants and joint venture entities) and its employees.

## 7. Dispensation

Any deviation from this policy should be requested by the Company's Compliance Officer for Group Chief Compliance Officer's approval. The written request for deviation from this policy will only be considered where the request details the solid reasons for why a deviation should be permitted and (if applicable) the alternative approach to be considered. Any suggested alternative approach should be based on a prudent, robust, and practical risk assessment based on the risk profile for the respective BU.



## Appendix 1 Roles and Responsibilities

Board is responsible for:

- Establishing the cultural values of integrity and fostering a culture of integrity where bribery and corruption are unacceptable;
- Committing to prevent bribery by persons associated with the Company; and
- Determining appropriate governance framework and business value and disseminating through the Company.

The Board delegates responsibility for compliance by the Company with applicable ABC law and regulation to the CEO.

CEO is responsible for:

- Communicating the Company values, setting the appropriate tone and ensuring staff understand their responsibilities;
- Responsible for the Company compliance with the Company policy, local laws and regulations and overseeing the implementation of the Programme and appropriate controls;
- Appointing a suitable ABCO who has adequate resources, autonomy and a reporting line to appropriate senior management;
- Allocating sufficient resources to the Programme to achieve compliance with the Company Policy; and
- Taking the appropriate disciplinary and/or any required remedial actions in the event of a breach.

The CEO may delegate responsibilities to appropriate Executives and functions but retains ultimate accountability for compliance with the Company Policy and applicable local law and regulations. The CEO may delegate responsibilities to his Executive and/or functional teams but should ensure that there are clearly defined lines of responsibility and delegated authority.

All employees are responsible for:

- Understanding and complying with the Company Policy and local regulatory requirements;
- Completing mandatory ABC training in a timely manner; and
- Escalating concerns of potential breaches of the Policy or ABC related regulations to management and/or local Compliance directly or via the whistleblowing channel.

Chief Corporate Governance Officer is responsible for:

- Providing regulatory advice to the CEO and Board on ABC risks and regulations;
- Designing and overseeing the Programme across the Company; and
- Maintaining the Company Policy and providing assurance to the Board (and its Committee) on its Company wide implementation.

Corporate Governance Committee is responsible for:

- Recommending the Company overall risk appetite and tolerance to the Board;

- Overseeing and advising the Board on future risk exposures and strategic risks;
- Reviewing Policy and recommending to the Board for approval;
- Providing oversight and supporting the implementation of the ABC Programme; and
- Supporting the Board and management in embedding and maintaining a supportive culture in relation to the management of risk.

Audit Committee is responsible for:

- Reviewing the framework and effectiveness of the Company's systems of internal controls;
- Reviewing regular reports from management and the results of any internal and external audits and monitoring to ensure that the necessary enhancements are made; and
- Monitoring the effectiveness of internal control and risk management systems, including compliance arrangements.

Compliance is responsible for:

- Designing and overseeing the Company-specific Programme, addressing both Group Policy and local law and regulations;
- Developing and maintaining appropriate and proportionate standards and guidance, and communicating these;
- Providing guidance and support on ABC matters within the Company and assisting Senior Management in identifying and managing bribery and corruption risks;
- Providing training to staff; and
- Ensuring appropriate and timely escalation of breaches to relevant senior stakeholders.

Legal is responsible for:

- Providing advice and support on ABC contract clause(s); and
- Providing advice and support to Compliance on the ABC-related law and regulations.

## Appendix 2 Red Flags and Risk Events for Bribery & Corruption

FWD requires business units to remain vigilant against bribery and corruption. In addition, subsidiaries in different jurisdictions are required to manage their respective bribery and corruption risks using localised red flags due to local culture and business practices.

While each transaction or counterparty should be evaluated on its specific facts, there are several red flags that may raise concerns. The list below is not intended to be exhaustive and is provided to prompt you to be diligent:

- You become aware that a third party engages in, or has been accused of engaging in, improper business practices;
- You become aware that a person in position of authority abuses his authority for personal gain;
- A third party insists on receiving a commission or fee payment before committing to sign up to a contract with us, or carrying out a government function or process for the company;
- A third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;
- You learn that a third party has a reputation for paying bribes, or requiring that bribes are paid to them, or has a reputation for having a 'special relationship' with government officials;
- You are asked to unnecessarily involve government officials outside of what is required;
- The third party has been subject to previous enforcement action for corruption related offences;
- A third party requests an unexpected additional fee or commission to 'facilitate' a service;
- A third party or government official demands entertainment or gifts before commencing or continuing contractual negotiations or provision of services;
- A government official requests that you provide employment or some other advantage to a friend or relative;
- You receive an invoice from a third party that appears to be non standard or customised;
- You notice that we have been invoiced for a commission or fee payment that appears large given the service stated to have been provided;
- You are offered an unusually generous gift or offered lavish hospitality by a third party;
- You are asked to give hospitality to persons who are not associated with the organisation (for example family members);
- You are asked to provide forms of gratification in exchange of promotion opportunities or sales leads;
- The third party requests a split of purchases to avoid procurement thresholds;
- A Government Official insists on a specific person or company to serve as third party;
- The third party requests you not to report or disclose a particular activity or transaction;
- An unnecessary middleman is involved in the contract or negotiations, and his addition has no obvious value to the performance of the contract;
- The third party business structure is unusual or overly complex with a lack of transparency;
- The third party requests for payment arrangements that might possibly violate local laws such as payment in another country's currency.



# Data Privacy Policy

## FWD Cambodia

Document ID	KH-COM-PO-0005	Document type	Policy
Issued by / Owner	Chief Corporate Governance Officer	Approved by	Corporate Governance Committee
Target audience	FWD Cambodia management, employees and contingent workers at all levels		
Document status	In-effect	Date last approved	22 June 2023

### Document approval history

Ver	Date Approved	Description
1.0	20 Oct 2021	First Version
2.0	22 Jun 2023	Revising based on new Group Version and format also was changed to comply with new Brand Policy

## Contents

1. Introduction.....	3
2. Scope.....	3
3. Personal Data.....	3
4. Roles and Responsibilities.....	4
4.1. Board of Directors .....	4
4.2. Corporate Governance Committee .....	5
4.3. Senior Management .....	5
4.4. Data Protection Officer .....	5
4.5. Compliance .....	5
4.6. Employees and Intermediaries.....	6
5. The Privacy Principles.....	6
5.1. Data Collection.....	6
5.2. Notification.....	7
5.3. Purpose Limitation.....	7
5.4. Adequacy and Relevance .....	7
5.5. Accuracy .....	7
5.6. Retention.....	7
5.7. Access and Correction .....	8
5.8. Security .....	8
5.9. Transfer .....	8
6. Privacy Impact Assessment .....	9
7. Record Keeping .....	10
8. Training and Awareness.....	10
9. Data Breach Incidents.....	10
10. Compliance Reporting .....	10
11. Definition.....	11
12. Review of this Policy .....	12
13. Dispensation.....	12

## 1. Introduction

FWD Life Insurance (Cambodia) Plc (“FWD or FWD Cambodia”) is fully committed to maintaining the integrity of personal data of our customers, employees, business partners, third parties or any other party whose data FWD controls. We respect data privacy and safeguard the data entrusted to us. Furthermore, we strive to comply with applicable privacy laws and regulations of jurisdictions from which the personal data is processed. As such each employee bears a personal responsibility for complying with this Policy in the fulfilment of their responsibilities and obligations in FWD.

This Data Privacy Policy (“Policy”) thus, outlines our commitment to respecting data privacy and provides guidance on how personal data should be collected, used, stored, transferred and disposed of by FWD. It also clarifies relevant roles and responsibilities, privacy principles and operational controls to protect personal data and minimise privacy risks.

This Policy should be read in conjunction with the [Code of Ethics and Business Conduct](#), the [Group AI and Data Governance Policy](#), the [Incident Management Policy](#), the [Group Data Protection Standard](#), the [Data Privacy Standard](#), [Group Data Retention and Disposal Management Guideline](#) and other relevant group policies, which have been referenced throughout the different sections of this policy.

## 2. Scope

This Policy establishes the general approach as well as the minimum standards to which FWD must adhere to. It applies to all FWD employees, contingent workers, contractors, temporary staff, business partners and data processors that process personal data on behalf of FWD. All employees and contingent workers must abide by this Policy and applicable data privacy laws and regulations. Any breaches in data privacy may expose FWD to civil or criminal penalties as well as reputational damage.

## 3. Personal Data

Personal data or personal identifiable information (“PII”) refers to any data, whether by its own or with other data, from which it is reasonably practical for the identity of an individual to be directly or indirectly ascertained.

Distinction shall be made on certain special categories of data that are considered particularly sensitive such as those revealing a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data or data concerning health or a natural person’s sex life or sexual orientation. Personal data categorized as sensitive in nature requires a higher degree of protection prior to processing. This is due to the nature of such

data, and because processing may be deemed too intrusive and could create significant risks to fundamental rights and freedom.

The below outlines some examples of personal data (without limitation):

Personal data	Sensitive personal data
<ul style="list-style-type: none"> <li>• Name of individual</li> <li>• Demographic information (e.g., gender, age, date of birth, marital status, occupation)</li> <li>• Contact information (e.g., address, personal phone number, personal email address, work phone number, work email address)</li> <li>• Policy information (e.g., policy number, claims details)</li> </ul>	<ul style="list-style-type: none"> <li>• Government-issued identity document and number (e.g., national identity card, passport, driver license)</li> <li>• Nationality and data revealing racial or ethnic origin</li> <li>• Health information, including medical, dental, pharmaceutical, genetic and biometric data (e.g., facial image, tone of voice, fingerprints)</li> <li>• Bank account, credit card number and other financial information (e.g., annual income, credit rating)</li> <li>• Surveillance and closed-circuit television (“CCTV”) recordings</li> <li>• Information related to sexual orientation, political opinion, religious belief and trade union membership</li> <li>• Information related to criminal record, conviction and allegation</li> </ul>

All personal data or PII is considered as “C3 – confidential” or higher as defined in the [Group AI and Data Governance Policy](#).

## 4. Roles and Responsibilities

### 4.1. Board of Directors

The Board of Director (“Board”) has oversight of the overall compliance with data privacy requirements. By demonstrating its commitment in establishing an effective internal control system in compliance with local legislation and related regulatory guidelines on data privacy, the Board plays a critical role in setting a data privacy culture. To fulfil its duties, the Board must be kept informed of timely information from senior management.

#### 4.2. Corporate Governance Committee

The Corporate Governance Committee (“CGC”) is accountable for approval of this Policy and directs the development and maintenance of minimum standards, guidelines and procedures pertaining to this Policy. The CGC has delegated the day-to-day responsibility for overseeing and implementation of this Policy to Compliance function.

#### 4.3. Senior Management

Senior management has responsibility for ensuring an effective implementation of Privacy Compliance Programme that is in accordance with this Policy, including:

- incorporating the requirements of this Policy into operational procedures as applicable;
- requesting advice from Group Compliance on any exception, deviation and waiver requests; and
- designating an individual or individuals at senior management level within the Compliance function as the Data Protection Officer (“DPO”), preferably the Head of Compliance or to be agreed with Group Compliance; or any person holding the necessary credentials or seniority level as may be required by local regulations. Chief Digital and IT Officer is designated as the DPO of FWD.

#### 4.4. Data Protection Officer

The DPO is responsible for:

- overseeing the localisation and implementation of this Policy and the Privacy Compliance Programme;
- informing and advising senior management and employees of their obligations in relation to the Policy;
- keeping up to date on data privacy matters;
- providing advise on privacy enquiries, complaints and access requests;
- coordinating with relevant departments in the event of privacy inspections, queries or visits by external parties or regulatory authorities; and
- providing advice on data protection impact assessments.

#### 4.5. Compliance

The Compliance function shall have oversight of all activities relating to data privacy, including:

- monitoring for compliance with this Policy and applicable laws and regulations;
- informing senior management of emerging data privacy risks and compliance initiatives, as well as identified compliance deficiencies and corrective action taken;



- assisting functional units in conducting privacy impact assessments on any projects, systems, tool, processes or enhancements prior to launch or roll-out;
- providing appropriate training to all relevant employees, in particular for employees engaged in any activity in relations to data privacy;
- taking appropriate action when breaches of this Policy are identified; and
- acting as the main point of co-ordination with the local regulatory body.

#### 4.6. Employees and Intermediaries

All employees and intermediaries play a vital role in ensuring personal data is properly safeguarded and must comply with applicable local laws and regulatory requirements. All employees and intermediaries acting on behalf of FWD must ensure that the collection, processing, using, disclosing, retaining and destruction of personal data are consistent with this Policy. A periodic data privacy risk assessment using a risk-based approach is to be conducted to assess potential privacy impact when new procedures involving personal data are implemented or when changes are made to such processes.

Any data privacy breach or incident identified must be reported to the Compliance function in accordance with the [Incident Management Policy](#) and the DPO will be advised.

## 5. The Privacy Principles

Data privacy relates to the appropriate collection, processing, use, retention, disclosure and disposal of personal data that has been provided or entrusted to a party according to the agreed purposes. The privacy principles provide a privacy guidance and serves as the basis in protecting the rights of data subjects whose personal data has been provided to FWD. The privacy principles are:

### 5.1. Data Collection

Personal data should be obtained by fair and lawful means, with the knowledge or consent of the data subject including circumstances where the personal data is to be shared with another party. There should be legitimate reasons for collecting and sharing of personal data, which is to occur in an open and honest manner. Personal data should be handled in a way that is reasonably expected and in a lawful way.

Where consent for specific use is required, such consent should be obtained separately and purpose for its collection should be specified in the privacy notification.

Where applicable, opt-in approach shall be preferred, particularly in marketing activities. Thus, FWD shall establish procedures to check against the opted-out list or a Do-Not-Call (“DNC”) register, to ensure that all marketing activities are only addressed to those persons who have provided opt-in consents.

## 5.2. Notification

The individual whose personal data is being obtained must be notified at time of collection on the purpose for which the personal data is collected, processed, used, retained, and disclosed.

The privacy notification must be clear and easy to understand and where required, must be tailored to cover specific purposes.

### 5.2.1 Cookies and Tracking Technologies

FWD should provide transparent Cookie Policy to any person accessing any FWD website, explaining the types of data the cookies collect and the purpose.

In the event third-party cookies are used in FWD website, it should state the types of information for which the cookies collect, to whom the information may be transferred and for what purpose.

## 5.3. Purpose Limitation

Personal data should only be obtained and used for specified purposes. The purposes must be considered appropriate under the circumstances by a reasonable person. In the event that the use of the personal data is not in line with the original specified purposes, it is not to proceed until consent from the individual has been obtained on such change of purpose with the exception of complying with relevant authority of law.

## 5.4. Adequacy and Relevance

Personal data should be adequate, relevant and not excessive to the purposes for which they are collected. As such, FWD should make reasonable efforts in data minimisation and only collect personal data necessary to properly fulfil the purpose. If a piece of data is of supplementary nature, FWD should indicate clearly that it is optional for the data subject to provide.

## 5.5. Accuracy

Personal data shall be accurate and, to the extent necessary for those purposes, be kept up-to-date. FWD should take practical steps to verify accuracy of personal data and establish procedures to rectify any inaccurate, misleading or outdated data. For the avoidance of doubt, this excludes circumstances where inaccurate data is provided by the data subject or a third party and accurately recorded.

## 5.6. Retention

Personal data collected for any purpose should not be kept longer than is necessary for the purpose collected. Once personal data is no longer needed in fulfilling the purposes of processing, it should

be permanently disposed of or irreversibly anonymised, such that the data subject cannot be reidentified.

FWD shall follow the [Group Data Retention and Disposal Management Guideline](#) that provides for the retention period requirements for each type of data in compliance with local regulations and industry guidelines. Once the maximum data retention period is reached, the personal data is deemed to be disposed of and irretrievably anonymised. Where required, a system should be in place for a systematic approach to review and destroy data in both manual and electronic format.

For personal data shared with data processors or any other parties, adequate contractual arrangement should be in place to prevent prolonged data retention than necessary.

### 5.7. Access and Correction

Individuals whose personal data are held by FWD should have certain rights to request for access and correction of their personal data. FWD shall establish a process in handling access and correction requests. A reasonable fee may be charged to offset any administrative or actual cost incurred in handling such requests.

### 5.8. Security

Appropriate physical, technical and organizational measures should be taken against unauthorized or unlawful processing, use, modification or disclosure, accidental loss or destruction of, or damage to, personal data. This applies regardless of whether the personal data is processed electronically or in paper form. When personal data is not properly safeguarded, it can cause serious reputational damage to FWD and can compromise the safety and trust of individuals whose personal data is held by FWD. It is imperative to have appropriate security measures to prevent the personal data held by FWD from being compromised whether accidentally or deliberately.

Before introducing any new system, tool, process or enhancements thereof, appropriate physical, technical and organizational measures to protect personal data must be defined and implemented. Consultation with the Chief IT and Digital Officer, Chief Legal and Compliance Officer, DPO and any other relevant personnel on said measures may be conducted. Furthermore, owners of the system, tool or process must ensure that the requisite IT security and data privacy assessments are conducted and that the necessary requirements and actions are addressed before the production launch. Production personal data, unless irretrievably anonymised, shall not be used as test data in non-production environments.

Security measures in place must be reviewed continually in order to adapt to changing regulatory landscape, technical developments or any physical or organizational changes. Refer to the [Data Protection Standard](#) for details of security requirements for handling of confidential data.

### 5.9. Transfer

Personal data shall only be transferred to a territory which holds the same level of protection in relation to personal data as the originating territory. Where such measures are deemed inadequate,

express consent must be obtained from the individual prior to transfer provided that it is permissible under local regulation.

When personal data is transferred to a third party, to process, use or disclose on behalf of FWD, care should be taken whereby the third party must uphold the same level of security measures in protecting the personal data to the same degree as if the work is performed by FWD. Reasonable steps must be taken by the user of the service provided by the third party to check that those security measures are in place and there must be a written contract setting out the scope of work performed by the third party including safe handling and erasure of the data.

### 5.9.1. Cross-border Transfer of Data

Where cross-border transfer of data is made, whether through the use of cloud technology or other means, the following steps must be considered to ensure protection of the data:

- Understand and comply with the local privacy laws and regulations and other legal requirements. If there is any prohibition on cross-border data transfer by local regulations, FWD must not provide the data outside of its country.
- Ensure data security measures and IT risk assessments have been conducted and reviewed by the appropriate teams (e.g., Information Security, Operational Risk, Compliance teams).
- The receiving country should hold an adequate level of protection in relations to personal data. Factors to consider may include the existence of data privacy law and independent supervisory authorities.
- Data protection controls must be commensurate with the classification of data based on the result of risk assessment. When necessary, explore data anonymisation or masking solutions or encryption technologies and tools.
- Where required by local regulations, obtain the necessary clearance from the regulator prior to the cross-border transfer or use of cloud platforms.

## 6. Privacy Impact Assessment

Before introducing any new or changes in projects, processes or systems that involve personal data of FWD stakeholders, a Privacy Impact Assessment (“PIA”) should be conducted. The assessment is designed to evaluate the privacy risks of a processing activity, minimise any adverse impact, and ensure appropriate safeguards are put in place. Examples of processing activities requiring a PIA include (without limitation):

- Commencement of any new projects or initiatives that involve personal data;
- Implementation of systems or tools that process personal data;
- Engagement with third parties with whom FWD will be sharing personal data; and
- Significant changes in projects, processes and systems that involve personal data.

PIA must be conducted at the planning phase of an initiative or project. This allows privacy risks to be identified upfront and key privacy principles to be incorporated in the project or system itself, achieving privacy by-design.

## 7. Record Keeping

All customer identification records, transaction and account records, plus business correspondence must be kept and maintained so that they can be made available to the relevant authorities in a timely fashion.

To comply with Sub-Decree on Insurance (2021), personal data collected shall not be retained for longer than fifteen (15) years after the end of business relationship. For other types of data, reference may be made to the [Group Data Retention and Disposal Management Guideline](#) for the relevant retention period requirements.

## 8. Training and Awareness

All employees should receive general information on data privacy laws, regulations and internal policies through training sessions. New joiners should complete the training as soon as reasonably practicable after commencement of employment. Records of the trainings should be kept in line with local regulatory requirements.

Contingent workers, acting on behalf of FWD, equally are also to receive relevant training as stipulated in their respective contract of engagement. Records of the trainings must be kept in line with local regulatory requirements.

## 9. Data Breach Incidents

Upon discovery of incidents involving the unauthorised disclosure of or access to, or the accidental or unlawful destruction, loss, alteration of, personal data transmitted, stored or otherwise processed by FWD, including those originated from third parties, shall be immediately reported to Compliance. The necessary reporting to the Governance, Risk and Compliance (“GRC”) tool must also be made in accordance with the [Incident Management Policy](#).

All data breach incidents that may have material privacy impact, including regulatory sanction, adverse public media exposure, cyber-attack or any high-risk cases (e.g., customer complaints), must be escalated to Group Compliance without undue delay.

Furthermore, where local regulations require it, the necessary breach notification or reporting to the regulator must be made within the required period.

## 10. Compliance Reporting

Each BU shall include in their quarterly report to Group Compliance the status of its Privacy Compliance Program, which includes the following:

- A summary of key local data privacy requirements and any material changes in such requirements from the previous year, if any;

- A summary of the results of the entity’s annual data privacy risk assessment, including key findings and action plans arising therefrom; and
- A description of any regulatory examinations or audits (external or internal) undertaken, including key findings.

## 11. Definition

Board refers to the Board of Directors of FWD Cambodia.

Contingent worker refers to non-permanent staff who provide managed services to FWD and requires prior FWD permission to access any FWD data or systems. They may fall in any of the following categories:

- Independent consultant – engaged through a consultancy agreement and performs specific and non-BAU matters on behalf of FWD.
- Contractors – engaged through a fixed employment contract with a third-party agency.
- Third party service provider – engaged through an employment contract with FWD-engaged service providers.

Data controller is a party which controls the processing of personal data through decision-making power over what information is collected, or the purpose or extent of its processing.

Data owner is someone responsible for the functionality and use of the data, at the domain level and has a stake in ensuring that the data is properly defined and used throughout the enterprise. This role holds ultimate accountability and authority for the data (e.g., data quality) within the domain.

Data processor is a party, such as business partner or third-party service provider, who has access to or processes personal data on behalf of FWD.

Data Protection Officer (“DPO”) refers to the role who oversees the implementation of this Policy and the overall Privacy Compliance Programme.

Data subject is the individual who is the subject of the personal data.

Direct marketing refers to the offering or advertising of products or services, including communication or distribution of marketing materials to an individual.

Do-Not-Call (“DNC”) register is a register of individuals who do not wish to receive telemarketing messages via phone call, short message service (“SMS”) or fax.

Employee refers to anyone who is permanently, temporarily or contractually employed by FWD, which includes all Board members, contractors, interns and trainees.

Intermediaries refers to licensed insurance agents or brokers advising or arranging contracts of insurance provided by FWD.

General Data Protection Regulation (“GDPR”) is a regulation in European Union (“EU”) law on data protection and privacy in the EU and the European Economic Area, which came in effect since 25 May 2018.

Governance, Risk and Compliance (“GRC”) refers to the Archer and/or ServiceNow which is applied to structure governance, risk management and regulatory compliance.

Third party refers to any supplier, vendor, consultant, sub-contractor or provider, whether an individual or an entity, providing goods or services to FWD.

Personal data and Personal Identifiable Information (“PII”) are interchangeable. It refers to any data, whether by its own or with other data, that identifies a data subject.

Personal Information Protection Law (“PIPL”) of the is the data privacy law in China, which came in effect since 1 Nov 2021.

Personal Data (Privacy) Ordinance (“PDPO”) is the privacy ordinance in Hong Kong, which came effect since 1994 with major amendments in 2012.

Privacy Compliance Programme (“PCP”) refers to the structured programme for privacy management by FWD. Refer to Section 8 for more details.

Sensitive personal data is a subset of personal data. It is a special category of data that are considered particularly sensitive, such as those revealing a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation. Personal data categorized as sensitive in nature requires a higher degree of protection as the context of their processing is deemed intrusive and could create significant risks to the fundamental rights and freedoms of a data subject.

## 12. Review of this Policy

This Policy is subject to review from time to time or at least every two (2) years to keep abreast with applicable legislative and regulatory requirements by Group Compliance.

## 13. Dispensation

Any deviation from this Policy should be requested by Chief Legal and Compliance Officer for Group Chief Compliance Officer’s dispensation. The written request of dispensation will only be considered where the request details the solid reasons for the use of alternative approaches will provide more prudent, robust and practical result of an assessment of the risk profile for the respective BU.

=== End of Document ===

C2 - Internal



# FWD Cambodia Whistleblower Policy

Document ID	KH-COM-PO-0011	Document Type	Policy
Issued by /Owner	Chief Legal & Compliance Officer	Approved By	Audit Committee (“AC”)
Target Audience	All management, employees and contractors at all levels		
Document Status	In-effect	Effective Date	3 August 2022

## Document Approval History

Version	Date Approved	Description
1.0	3 August 2022	First Version



## Table of Contents

1. Introduction and scope .....	3
2. Roles and responsibilities .....	3
3. Types of matters to report.....	4
4. Reporting of concerns .....	5
5. Anonymity.....	6
6. Non-retaliation .....	6
7. Investigation procedures.....	7
8. Reporting .....	7
9. Review of the policy .....	8
10. Communication of the Whistleblower Policy .....	8

## 1. Introduction and scope

This policy applies to all personnel and contractors (hereinafter referred to as the “Employees”) of FWD Cambodia (“FWD”) and third-party business partners. FWD is committed to conducting business with the highest standard of integrity and fairness and with respect to our values and applicable laws and regulations.

A culture of honesty and integrity includes our ability to speak up when we feel that something is wrong. If ever we observe or suspect a violation of our Code of Ethics and Business Conduct or something that may be a threat to our integrity and our reputation, this Whistleblower policy covers the confidential, secure and if necessary, anonymous way to report concerns so that management can take appropriate action.

FWD recognizes that reporting observed, or suspected misconduct is essential to sustain our brand, reputation and ability to operate. Thus, we do not tolerate any form of retaliation, harassment, reprisal or adverse employment consequence against someone who makes a report in good faith.

## 2. Roles and responsibilities

A Whistleblowing Panel (WB Panel) shall be formed for the purpose of processing, investigating and determining the genuineness of any whistleblower report or complaint received and recommend appropriate actions to be taken based on FWD’s Disciplinary Guidelines. At the minimum, the following may comprise the WB Panel:

- Chief Financial Officer (CFO);
- Chief People & Culture Officer (CPCO);
- Chief Legal and Compliance Officer (CLCO);
- Head of Internal Audit (HOIA); and/or
- Other relevant resource persons as may thereafter be identified by the WB Panel.

Should the report or complaint be related to the functions led by the member of the WB Panel, they will be excluded from notification and the investigation process.

The Legal and Compliance Manager (LCM) shall act as the Secretary of the WB Panel.

Management must promote the policy to ensure that everyone knows that they are able to raise concerns without fear of reprisals. All employees, contractors and third-party business partners should ensure that they take steps to disclose any misconduct or malpractice of which they become aware. If there is ever any question about the contents or application of this policy, the CLCO should be contacted.

### 3. Types of matters to report

The whistleblower procedure does not replace the reporting channels that are in place such as via manager, HR or Compliance but rather is an additional channel which can be used if required. The types of matters that can be reported in line with this policy cover a broad range of matters. The following are some examples:

- 3.1. questionable accounting, internal accounting controls, or auditing matters (collectively referred as “**Accounting Allegation**”), including, without limitation:
  - 3.1.1. fraud or deliberate error in the preparation, review or audit of financial statements of the Company;
  - 3.1.2. fraud or deliberate error in the recording and maintaining of the Company’s financial records;
  - 3.1.3. deficiencies in, or non-compliance with, the Company’s internal control over financial reporting;
  - 3.1.4. misrepresentation or false statements regarding a matter contained in the Company’s financial records, financial statements, audit reports or any filings made with the Securities and Exchange Commission (including periodic or current reports);
  - 3.1.5. deviation from full and fair reporting of the Company’s financial condition and results;
  - 3.1.6. substantial variation in the Company’s financial reporting methodology from prior practice or from generally accepted accounting principles;
  - 3.1.7. issues affecting the independence of the Company’s accounting firm; and
  - 3.1.8. falsification, concealment or inappropriate destruction of corporate or financial records
- 3.2. legal or other allegations (collectively referred as “**Conduct Allegation**”), including, without limitation:
  - 3.2.1. breach of laws, regulations, license provisions or relevant securities laws;
  - 3.2.2. violation of FWD’s Code of Ethics and Business Conduct, business principles or policies;
  - 3.2.3. suspected bribery or other corruption, fraud, money laundering, financial irregularities, information security breaches, suspicion of malpractice that may cause reputational damage to the FWD brand;
  - 3.2.4. unethical behaviour or unfair treatment at work or discrimination;
  - 3.2.5. human rights violations; and/or
  - 3.2.6. environmental, health and safety issues which could have a significant adverse impact on FWD;

- 3.3. alleged retaliation against employees and other persons who make, in good faith, Accounting Allegations or Conduct Allegations (“**Retaliation Allegation**”).

The whistleblower reporting channels are designed to provide an alternative way to raise a matter where there is a reservation about using other channels.

## 4. Reporting of concerns

Whistleblowers can report their concerns:

- By calling the **Speak Up Hotline**: (HK tollfree) 800 903 375; (SG tollfree) 3158-7652.

The call will be answered by a specialist and independent third party operator (**Convercent**) and is completely confidential. The whistleblower can choose to remain anonymous if required and the call is not voice recorded. All reports received via Speak Up Hotline will be logged to the Speak Up Online by the independent third-party operator for follow-up action and management.

The Speak Up Hotline (tollfree) for the other countries where FWD operates are as follows:

- Cambodia - 239-62515
- China - 400-120-0253
- Indonesia - 021-29223057
- Japan - 0800-100-0081
- Macau - 6262-5093
- Malaysia - (0)1548770361
- Philippines - 2-86263210
- Singapore - 3158-7652
- Thailand - 021056128
- Vietnam - (028) 44581010

- By submitting an online report via **Speak Up Online**<sup>1</sup> through the following links:

- [www.fwd.com/SpeakUp](http://www.fwd.com/SpeakUp)

Whistleblowers are able to complete a reporting form in their own time and in their chosen language using their smartphone, tablet or PC from anywhere in the world.

- By sending an email addressed to the Chairman of the Group Audit Committee (“GAC Chairman”) or such other designated member of management to the following address:
  - [GOSpeakUp@fwd.com](mailto:GOSpeakUp@fwd.com)

<sup>1</sup> Speak Up Online is multi-lingual and option to change the language is available in the site.

All whistleblower reports should be factual rather than speculative or conclusory and should contain as much information as possible, including attachment of supporting documents, if available, to allow proper assessment. Further, all reports should at least contain names of individuals suspected of violations, the relevant facts of the violations, how the person became aware of the violations, any steps previously taken by the person/whistleblower, who may be harmed or affected by the violations and, to the extent possible, an estimate of the misreporting or losses to FWD as a result of said violations.

Where reports are submitted through the Speak Up Online, whistleblowers can check on the progress of an investigation using their case ID and password, which is issued when they first submit a report. This allows a whistleblower to be updated with the progress if appropriate and to respond to additional questions while remaining anonymous.

Whichever reporting channel the whistleblower decides to use to report, the whistleblower's identity will remain anonymous if they wish. The third party vendor will not attempt to trace the whistleblower's details at any time and should the whistleblower volunteer their details, the third party vendor will not pass them on to FWD unless the whistleblower gives them their explicit permission to do so.

## 5. Anonymity

To encourage the whistleblower to report without fear of retaliation and to safeguard the confidentiality of the matter and the whistleblower, whistleblowers may raise the matter anonymously, as stated above.

Also all reports prepared will not include the name of the whistleblower. The identity of the whistleblower will only be revealed:

- To the investigation team if needed to facilitate the investigations (please refer to Section 8 for details); or
- As required by law.

Apart from the abovementioned situation, if the investigation team at some point is required to report the name of the Whistleblower, the investigation team will obtain the Whistleblower's consent before disclosure, unless the investigation team has lawful reasons not to do so.

## 6. Non-retaliation

Taking actions to protect FWD's integrity is everyone's responsibility and we encourage all employees and contractors to be vigilant about it.

We will not retaliate against anyone who, in good faith, seeks advice, raises a concern, or reports misconduct. Any employees engaging in retaliatory conduct will be subject to disciplinary action, up to and including dismissal or termination of employment or appointment. If any employee suspects that they or another FWD employee has been retaliated against for raising a concern, they should contact the CLCO immediately.

For the avoidance of doubt, neither FWD, the AC, WP Panel nor any director, officer, employee, contractor, subcontractor, or agent of FWD shall dismiss, terminate, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate or retaliate against any person who, in good faith, makes a report to or otherwise assists the AC, WB Panel, management or any other person or group, including any governmental, regulatory or law enforcement body, in investigating a concern or a report. These prohibitions also apply to FWD's subsidiaries and affiliates whose financial information is included in the consolidated financial statements of FWD.

## 7. Investigation procedures

Investigation procedures are detailed in the [Investigation Procedures](#) document.

All reports received will be acknowledged through Speak Up Online with a request to the whistleblower to check the system frequently should further information is required during the course of the investigation.

Every report received is evaluated and where appropriate, investigated upon. Where after preliminary evaluation a full investigation is deemed to be not necessary, e.g., report contains unspecified and broad allegations without appropriate supporting evidence attached, report is not credible, etc., the matter shall be deemed closed without further action.

Where circumstances warrant, the CLCO shall escalate a concern or report received to the AC Chairman for evaluation, e.g., matters with potential adverse effect on the Company's reputation or financial statements, etc.

Upon completion of any investigation, the following are the possible resolutions made pursuant to this policy:

- a. Allegations made have not been substantiated;
- b. Allegations made have been partially substantiated with appropriate corrective action taken; or
- c. Allegations have been fully substantiated with appropriate disciplinary or corrective action imposed against the erring employee or officer.

Final resolution of the case will be uploaded into Speak Up Online on a confidential basis. Details on the actions taken by the company or copy of the report may be shared with the whistleblower subject to the WB Panel approval and applicable laws.

## 8. Reporting

The CLCO shall, at every AC meeting, present a summary of all of the reports received by, or forwarded to, them (including those reports that they decided not to investigate) and all the material developments, findings and conclusions of investigations since the previous meeting. The AC may or may not accept such findings and conclusions. The CLCO shall likewise

provide such additional information regarding any report or investigation as may be requested by the AC.

The CLCO shall maintain a register for all reports received and investigated on under this Policy for a period of seven (7) years, unless otherwise notified by the GC of an extended retention period. Further, upon expiration of the retention period, including any extended retention period, and with the consent of the GC or where purpose for obtaining such information and documents has ceased, the CLCO shall cause the deletion and disposal of all information and documents in relation to a whistleblower report.

All documents obtained pertaining to whistleblower reports shall be generally classified as “C3-Confidential” as prescribed under the FWD Information Classification and Handling Standard. Nevertheless, should circumstances warrant, it will be classified as “C4-Restricted”.

## 9. Review of the policy

The Whistleblower Policy will be reviewed annually AC.

## 10. Communication of the Whistleblower Policy

Compliance is responsible for communicating these sections of the policy and ensuring that all FWD employees know that FWD has a Whistleblower Policy, program and process.

== End of Document ==

C2 - Internal



## FWD Cambodia

# Compliance Charter and Management Policy

Document ID	KH-COM-PO-0014	Document type	Policy
Issued by / Owner	Chief Legal & Compliance Officer	Approved by	Corporate Governance Committee ("CGC")
Target audience	All management, employees and contractors.		
Document status	In-Effect	Date last approved	27 June 2022

### Document approval history

Version	Date approved	Description
1.0	27 June 2022	First Version



## Contents

1.	Introduction and Scope.....	3
2.	Compliance Charter.....	3
2.1	FWD Compliance Mandate .....	3
2.2	FWD Group Compliance Mission .....	4
2.3	FWD Group Compliance Vision.....	4
2.4	Purpose of the Compliance Function at FWD.....	4
3.	Compliance Risk .....	4
4.	Roles and responsibilities for Compliance Risk Management .....	6
4.1	Group Chief Compliance Officer (“GCCO”) and Group Compliance .....	7
4.2	Chief Legal & Compliance Compliance (“CLCO”) and Compliance .....	8
5.	Compliance Management Process.....	10
5.1	Regulatory Obligations .....	10
5.2	Compliance Policies .....	10
5.3	Training, awareness and communication .....	11
5.4	Risk Assessments.....	11
5.5	Annual Compliance Plan (“ACP”).....	12
5.6	Compliance Monitoring.....	12
5.7	Compliance Management Information (“MI”) and Key Risk Indicators (“KRI”) Dashboards	13
5.8	Maturity Assessments .....	13
5.9	Compliance effectiveness .....	13
6.	Compliance Reporting .....	14
6.1	Group Compliance reporting.....	14
6.2	Compliance Reporting.....	14
7.	Outsourcing .....	15
8.	Review of this policy .....	15
9.	Dispensation .....	15

## 1. Introduction and Scope

Our business activities are highly regulated to varying degrees across the markets within which we operate, exposing us to a variety of inherent compliance risks. To minimise and manage these compliance risks, FWD is committed to the design and progressive implementation of a risk-based compliance management process across all of our businesses.

In line with our Code of Ethics and Business Conduct, we believe in “Doing the Right Things Right”. Compliance at its most fundamental level is simply about “Doing the Right Things Right”. Therefore, our approach to compliance is concerned with the quality of our practices and processes, ensuring that everyone at FWD knows, or knows how to easily find out, what is the right thing to do every day in every aspect of their, all playing a part in managing compliance risks.

The objective of the Compliance Charter and Management Policy is to establish FWD’s approach to managing compliance risks, ensuring there is a common approach across FWD. This policy should be read in conjunction with other relevant policies including the Regulatory Management Policy, Operational Risk Management Policy, and the Enterprise Risk Management Framework and Policy, which sets the overall framework for identifying and managing risks at FWD.

This policy applies to FWD Life Insurance (Cambodia) Plc (“FWD”).

## 2. Compliance Charter

The compliance charter describes the organisation, operation and roles and responsibilities for compliance management at FWD and requires the establishment of a Compliance function across the group.

### 2.1 FWD Compliance Mandate

The FWD Compliance Mandate is simple:

- We will comply with the requirements of the law, industry codes and standards not just because it is required but because it is the right thing to do.
- We will proactively identify compliance issues that impact our business and establish systems and processes to effectively and efficiently address these issues. This will include the development of a training, communication, monitoring, testing and reporting program for compliance risk management.
- We will ensure that we remain up to date with all regulatory developments that impact our businesses and that all new and revised requirements are assessed and embedded in an efficient and effective manner within the required timeframe.

## 2.2 FWD Compliance Mission

To create and maintain a risk-based approach to compliance management that aligns with the overall businesses strategic objectives and generates flexible and innovative solutions to achieve compliance requirements within the local operational context.

## 2.3 FWD Compliance Vision

To create a culture of integrity where:

Every FWD employee, contractor and sales representative in every location understands the role they play in protecting FWD's reputation and commits to doing the right thing not just because the law says so but because they believe it is the right thing to do for FWD and our customers.

## 2.4 Purpose of the Compliance Function at FWD

To build and embed a risk-based approach to managing compliance risks that:

1. Facilitates a culture that first and foremost prevents compliance issues and incidents from occurring. When prevention fails, facilitates the speedy detection of the issue and ensures rectification quickly and effectively as part of a continuous improvement process.
2. Identifies all the applicable compliance requirements and obligations for the company and the risks involved.
3. Effectively mitigates compliance risks by engaging the business at all levels and ensures employees know how to do the right things right by translating compliance requirements into policies, procedures, training and controls.
4. Supports a culture of integrity and trust which encourages active participation by employees to speak up and report compliance issues or concerns.
5. Monitors the effectiveness and efficiency of compliance procedures, controls and arrangements.
6. Facilitates strong, effective and trusting relationships with regulators and the industry.
7. Provides concise effective and efficient compliance reporting to senior management, committees and the Board.

## 3. Compliance Risk

As per the Group Enterprise Risk Management Policy, Compliance Risk is defined *as the risk losses from damage to reputation, legal or regulatory sanctions, financial loss or loss of license to operate which flow from failure or perceived failure to meet compliance obligations.*

All departments at FWD are exposed to various compliance risks. Whilst the Compliance function is responsible for overseeing compliance risks, there are some compliance risks that require specialist knowledge and these will be managed by relevant subject matter experts (e.g. employment laws and legislations, financial reporting and accounting standards, etc.).

At a minimum, the Compliance function should have oversight over the following compliance risks:

- Financial Crime Compliance (“FCC”) - Loss from any offence involving handling money or property that is from the proceeds of crimes or financing terrorism; the abuse of entrusted power for gain by offering (or promising to offer) or receipt of anything of value; failing to report the tax residence status; from any misconduct in or misuse of information related to a financial market.

Money Laundering & Terrorist Financing

- Insufficient KYC documentation/update such as customers, 3rd parties, and vendors
- Inadequate name scanning
- Transaction monitoring failures
- Suspicious transaction and large cash transaction report filing failure

Corruption & Bribery

- Inaccurate reporting on in scope activities such as gifts & entertainment, incentive, sponsorship, marketing events

FATCA/CRS

- Improper identification of customer’s tax status  
Inaccurate reporting for FATCA & CRS

Market Abuse

- Insider Dealing (by staff or Company)  
Failure to disclosing price sensitive information

- Conduct - Losses arising or adverse consequences due to conducting insurance business in a way that does not ensure the fair treatment of customers, fair outcomes, or results in harm to customers.

Distribution

- Unqualified and unfit distributors
- Inappropriate incentive schemes and remuneration structures
- Sales misconduct and poor quality sales (Mis-selling, misrepresentation, switching, churning, inappropriate replacement, poor advice and recommendations, etc.)
- Use of ambiguous and misleading marketing and product materials

Vulnerable customers

- Vulnerable customer not defined, identified and safeguarded

Product

- Unfair, ambiguous and misleading product design, features, terms and conditions, and exclusions
- Failure to identify appropriate target customers and segmentation
- Poor value for money (unfairly priced, poor product value proposition etc.)
- Product pricing errors
- Failure to perform product portfolio reviews

- |                              |  |
|------------------------------|--|
| Post sales customer outcomes | <ul style="list-style-type: none"> <li>• Failure to process and manage claims resulting in unfair customer outcomes</li> <li>• Failure to address customer complaints resulting in unfair customer outcomes</li> <li>• Poor after sales service and customer communications</li> </ul> |
| Organisational culture       | <ul style="list-style-type: none"> <li>• Poor ‘tone from the top’</li> <li>• Poor staff engagement</li> <li>• Poor demonstration of our brand values</li> <li>• Breaches of the Code of Ethics and Business Conduct</li> </ul>   |
| Conflicts of Interest        | <ul style="list-style-type: none"> <li>• Unmanaged structural conflicts of interest</li> <li>• Unmanaged personal conflicts of interest</li> </ul>   |
- 
- Regulatory - Losses arising or adverse impact to business operations from:
    - Breach of regulation or industry practices and codes
    - Fines and sanctions imposed by the regulator
    - Ineffective and non-transparent relationship with regulators
    - Failure to effectively implement regulatory changes
    - Failure to effectively implement issues and findings raised by regulators
    - Improper licensing, certification and/or registration
  - Privacy - Losses arising from
    - excessive collection of personal data not required for the primary purpose
    - unauthorised processing of personal data not required for the primary purpose
    - unauthorized disclosure of personal information
    - outdated personal data on record
    - unnecessary retention of data
    - unsecured transfer of personal data
    - unauthorised cross-border transfer of personal data
    - improper destruction or disposal of personal data
    - insufficient response to data breach incident

For further details of the operational risk taxonomies, please refer to the Group Operational Risk Management Policy.

## 4. Roles and responsibilities for Compliance Risk Management

Establishing effective governance over compliance risk is necessary to ensure a strong compliance culture within the organisation. At FWD, as per the Enterprise Risk Management Framework, we implement a three lines of defence model to managing risks. This model is based on the fundamental principle that the business owns and is responsible for the effective management of its compliance risks. Refer to the Enterprise Risk Management Framework for further details.

Compliance functions work in partnership with the business to ensure that major compliance risks are identified and mitigated with the right level of controls embedded within business processes and

operations. Compliance and business leaders are jointly responsible for ensuring that everyone understands that they have a critical role to play in building a culture of integrity and trust, and protecting the reputation of each other and of FWD.

#### 4.1 Group Chief Compliance Officer (“GCCO”) and Group Compliance

The Group Chief Compliance Officer manages the Group Compliance function, and is responsible for ensuring the Group Compliance function delivers and performs the following:

- Compliance management framework, strategic direction and culture
  - Set the strategic direction for the Compliance function across FWD ensuring that it is aligned to the business strategy
  - Establish an effective compliance management framework which assists FWD Group to meet its legal, regulatory and supervisory obligations
  - Develop and manage the Group Compliance annual plan and budget
  - Promote and sustain an effective compliance culture, and monitor the consistent and effective implementation of compliance arrangements and activities across FWD
  - Develop, maintain and advise on Group Compliance policies and minimum group standards, and recommend compliance policies for approval at relevant governance and Board committees
  - Effectively implement compliance management (including risk and control assessments, compliance monitoring and testing, compliance training, etc.) (refer to section 5 for further details)
  - Support and advise on key Group initiatives and projects
- Regulatory management
  - Manage the Group’s regulatory obligations list and ensure new / revised requirements are assessed and appropriately implemented
  - Keep abreast of regulatory and industry trends in the region and globally
  - Build and maintain relationships with Group supervisory regulators and local key regulators in jurisdictions where FWD operates
  - Refer to the Regulatory Management Policy for further details.
- Group Compliance Approval
  - In line with various Group Compliance policies (e.g. Gift and Entertainment and Anti-Bribery Policy, Conflicts of Interest Policy, Securities Dealing Policy etc.), provide Group Compliance approval, where required
  - Assess and approve policy dispensation requests from BU Compliance
- Reporting
  - Report to senior management and relevant Boards or committees on the key compliance and regulatory risks impacting the group, progress of the annual compliance plan, and the overall effectiveness of compliance management arrangements across the group (refer to section 6 for further details)

- People and collaboration
  - Coach, lead and develop Group Compliance members and BU HOC, ensuring there is continual professional development of compliance officers across the group
  - Ensure that there is a sufficiently resourced, qualified, experienced and skilled compliance officers in the Group Compliance function and in the BUs
  - Liaise with other governance functions including risk management, legal and audit to ensure an integrated approach to risk management
  - Build trusting relationships and partnerships with Group senior management and first line management to become trusted compliance advisors
- Oversight of BU Compliance functions
  - Work with BUs to assess the maturity of BU compliance processes and arrangements and develop roadmaps to improve
  - Review and advise on BU compliance policies and procedures, annual compliance plans, compliance issues and incidents, compliance risk assessments, compliance monitoring and testing, regulatory management, compliance reports, and other relevant topics, as appropriate
  - Develop and rollout compliance guidelines and templates to assist BUs with operationalising Group compliance policies
- Whistleblower investigations
  - The GCCO is the Reporting Officer for all whistleblower matters across group and is responsible for the management of the group-wide Convercent reporting system or Concern Online. The GCCO must ensure that all whistleblower matters are investigated in line the Whistleblower Policy and Procedures.
- Escalation
  - The GCCO must have the authority and obligation to inform the Chair of the Group Board (or relevant sub-committee) promptly and directly on material non-compliance by members of management or material non-compliance in the BUs where management are not taking the necessary corrective actions and a delay would be detrimental to group or its policy holders.

#### 4.2 FWD Chief Compliance Officer (“CCO”) and Compliance

FWD must appoint a CCO to lead the Compliance function. The Compliance function is directly responsible for managing compliance risks and ensuring policies and standards meet the requirements of the local regulators and the minimum standards defined in Group policies. The CCO is responsible for ensuring the Compliance function delivers and performs the following:

- Embed the compliance management framework in FWD, to ensure FWD complies with local regulatory obligations and minimum group standards

- Develop and execute the annual compliance plan once it has been agreed with local management and the GCCO, and approved by the relevant committee
- Promote and sustain an effective compliance culture, and monitor the consistent and effective implementation of compliance arrangements and activities at FWD
- Effectively implement compliance management (including risk and control assessments, regulatory obligations management, maturity assessments, compliance monitoring and testing, compliance training, etc.) (refer to section 5 for further details)
- Localise Group compliance policies and ensure they are implemented and operationalized to meet local regulatory requirements, business context and minimum group standards
- Provide compliance advice on regulatory compliance matters (e.g. new product launches, marketing materials and campaigns, establishment of new business relationships, mergers and acquisitions, sales process, sales misconduct investigations, distribution disciplinary actions, new systems and processes, projects etc.), and where required, provide compliance challenge and approval to ensure business decisions are in line with regulatory obligations
- Report to senior management, relevant Boards or committees, and Group Compliance on the key compliance and regulatory risks impacting FWD, progress of the annual compliance plan, and overall effectiveness of compliance risk management (refer to section 6 for further details)
- Keep abreast of regulatory and industry trends impacting FWD and the region
- Liaise with regulators and industry bodies and participate, where possible, in industry meetings to ensure knowledge exchange about regulations and to improve compliance risk management knowledge
- Assist with the investigation of whistleblower reports in line with the Whistleblower Policy and Procedures, when required
- Report incidents and issues to the management and the GCCO in accordance with the Incident Management Policy
- Coach, lead and develop Compliance staff, ensuring there is continual professional development of compliance officers
- Develop an understanding of the business strategy, practices and processes and build positive working relationships with the CEO and all members of the executive team to become the trusted compliance advisor
- Partner with Legal, other Risk Management functions, employees, management, relevant Boards and committees to ensure integrated risk management efforts



## 5. Compliance Management Process

The Compliance Management Process comprises of the key activities performed by the Compliance function to manage compliance risk. Each of the respective activities is described below.



### 5.1 Regulatory Obligations

FWD must comply with all relevant laws, regulations, and regulatory guidelines which govern its operations and license (collectively known as “regulatory obligations”), and be transparent, open and clear with our dealings with regulatory authorities.

FWD must maintain a list of key regulatory obligations which impacts their license and operations. Compliance is ultimately responsible for maintaining the obligations list and should closely work with the relevant departments, obligation/control owners and subject matter experts (where required), to ensure that the obligations list is kept up to date.

Refer to the Regulatory Management Policy for further details on how we should manage our regulatory obligations and relationship with regulatory authorities.

### 5.2 Compliance Policies

Compliance policies and procedures should be developed to ensure business processes and controls meet our regulatory obligations and the minimum standards set by Group Compliance.

At minimum, the following compliance policies and procedures must be in place:

- Code of Ethics and Business Conduct
- Compliance Charter and Management Policy
- Regulatory Management Policy
- Anti-Money Laundering (“AML”) and Counter Terrorist Financing (“CTF”) Policy

- Anti-Bribery and Corruption (“ABC”) Policy
- Data Privacy Policy
- Conflicts of Interest Policy
- Securities Dealing Policy
- Social Media Policy
- Customer Complaints Policy
- Whistleblower Policy and Procedures
- Distribution and Sales Quality Policy
- Treating Customers Fairly Policy
- Foreign Account Tax Compliance Act (“FATCA”) Policy

All policies are required to be approved by the Corporate Governance Committee (or equivalent). The Code of Ethics and Business Conduct, Customer Complaints, AML/CTF, and FATCA policy must also be approved by the Board.

### 5.3 Training, awareness and communication

All staff must be educated on compliance policies and procedures and their responsibility to comply with the relevant requirements.

Compliance function should develop an annual compliance training, awareness and communication plan, which includes induction training for all new joiners, and mandatory annual training for all staff, and where required the Board of Directors. Compliance must proactively monitor the completion of mandatory training courses and escalate overdue cases to direct reporting managers / senior management, to ensure that all necessary training is completed on a timely basis. Training completion must be recorded.

In addition to training, the annual plan must also include compliance communication and awareness initiatives. Some examples include the Compliance Fun Fair, newsletters, posters, quizzes, competitions and email communications.

### 5.4 Risk Assessments

A Risk Assessment for each key compliance risk area must be performed on at least an annual basis or when there are material changes to regulatory obligations. The results of the Risk Assessment should form the basis for compliance planning and understanding the monitoring activities that should be conducted. The Risk Assessment should be performed with the template developed by Group Operational Risk.

In addition to the annual Risk Assessment process, Compliance should assist 1st line management during the Key Controls Self-Assessment (“KCSA”) (or equivalent) exercise for business processes and controls which have a compliance impact. During this process, Compliance should assist with understanding the degree of exposure to key obligations and assess whether there are adequate business processes and controls to comply. Results of the KCSAs should feed back into the Risk Assessment of key compliance risk areas.

Please refer to the Group Operational Risk Management Policy for further information.

### 5.5 Annual Compliance Plan (“ACP”)

Compliance must develop an ACP that records the planned compliance initiatives and activities for the year. The ACP must be developed to address key compliance risks and must meet local regulatory requirements.

The Group ACP will set the strategic direction of the Compliance function across FWD. The BU ACP should be aligned to the Group ACP.

The ACP must be approved by the relevant committee. For FWD, the ACP must also be reviewed by and agreed with Group Compliance, prior to obtaining approval from the relevant BU committee.

### 5.6 Compliance Monitoring

Compliance monitoring is a broad topic which can cover ongoing surveillance, quality assurance (QA) and routine monitoring activities as well as detailed reviews such as thematic reviews, remediation reviews and regulatory change reviews. These can be performed at both the BU and Group level. Monitoring is central to the compliance plan, and FWD must develop a risk-based compliance monitoring plan that covers key compliance obligations and risks.

Monitoring should be performed on a recurring basis and on an ad-hoc basis for specified areas. The frequency of review and level of assurance will vary based on the level of risk, typically with higher risk areas reviewed more frequently.

Examples of types of monitoring:

- **BAU surveillance:** These are ongoing surveillance, QA and routine monitoring activities which are usually embedded within business processes. These can be performed by the 1<sup>st</sup> and/or 2<sup>nd</sup> line. Refer to the “Group Compliance Monitoring Toolkit”, which currently provides examples for Distribution and Sales areas. Note that the Toolkit will continue to be updated by Group Compliance to include other key compliance areas.
- **Thematic reviews:** These are specific deep dive reviews of key risks, business processes and/or obligations that seek to reassess control design effectiveness and/ or operating effectiveness. These reviews are typically performed by Group as it may also focus on revalidating controls and testing performed by the Compliance teams, however can also be performed by or together with Compliance teams. A thematic review may also be performed in response to a specific incident or breach, or at the request of a governance committee or senior management.
- **Remediation reviews:** These are post implementation reviews performed by Compliance which focuses on ensuring that deficiencies or non-compliance previously identified (from various sources, including testing and reviews, regulatory inspections, audit, incidents, etc.) have been appropriately remediated. Group Compliance should perform these reviews over higher risk areas

or significant regulatory breaches / non-compliance to ensure the company has appropriately actioned their remediation plans.

- Regulatory change reviews: These are post implementation reviews of significant regulatory changes to verify compliance.

Remediation and action plans should be developed for any findings identified from compliance monitoring. Results from compliance monitoring should be clearly documented, and key findings should be tabled to relevant committees. Any findings from compliance monitoring should be remediated timely.

### 5.7 Compliance Management Information (“MI”) and Key Risk Indicators (“KRI”) Dashboards

Compliance MI and KRI dashboards provide early indicators and signals of potential compliance issues (e.g. sales misconduct, non-compliance, potential money laundering, etc.). It also supports monitoring over key compliance risks and the assessment of compliance effectiveness. The Company and Group Compliance must work with the business to identify, monitor and report on MI and KRIs across compliance risks. MI / KRIs that trigger actions should be tracked and closely monitored.

### 5.8 Maturity Assessments

Group Compliance should design a maturity assessment model for all key compliance risks. The purpose of the maturity assessment is to understand the compliance arrangements including processes and controls in place at the BUs.

Compliance function should review and self-assess the maturity of their compliance arrangements on a periodic basis and submit the results with supporting evidence to Group Compliance. Based on the results of the maturity assessment, Compliance should develop a roadmap and actions to enhance applicable compliance processes.

Assessing the maturity of our compliance arrangements allows us to benchmark and set out a roadmap for development, and longer term planning for the overall Compliance function across FWD.

### 5.9 Compliance effectiveness

The effectiveness of the Compliance function must be measured on an ongoing basis. Maturity assessments, findings from compliance monitoring and testing, MI dashboards, KRIs, risk culture survey and KPIs are examples of ways the effectiveness of the compliance function can be measured.

The Compliance function should be continually assessed to ensure it remains relevant to the business and effective in managing compliance risks faced by FWD. Periodically, the Group Board may request independent assessment of the effectiveness of the Compliance function.

## 6. Compliance Reporting

One of the key responsibilities of Compliance function is to ensure that there is adequate reporting to senior management and the Board or committees on compliance and regulatory risks, and the effectiveness of the compliance processes in place. This ensures that there is effective oversight of compliance risks by management and the Board.

### 6.1 Group Compliance reporting

The Group Chief Compliance Officer should perform periodic compliance reporting to the Group senior management, Compliance Operational and Risk Committee (“CORC”), Group Risk Committee (“GRC”), Group Audit Committee (“GAC”) and the Group Board.

At a minimum, the following information should be reported:

Quarterly compliance reporting to CORC, GRC and GAC

- Compliance risk ratings across key compliance areas and commentary of significant factors contributing to the risk rating
- Compliance MI dashboards (inc. KRIs)
- Regulatory developments across the group and outlook
- Regulatory actions or inspections impacting the group
- Progress of the annual Group Compliance plan
- Key compliance initiatives across the group
- Material findings from compliance monitoring reviews, regulatory inspections, maturity assessments etc.
- Whistleblower cases (GAC only)

Quarterly compliance reporting to the Board

- Significant regulatory developments across the group

### 6.2 Compliance Reporting

Compliance function should perform periodic reporting to their senior management team, the CGC and relevant Board committees in line with local requirements and practices.

At a minimum, Compliance must report the following to Group Compliance on a monthly and quarterly basis:

- Regulatory developments impacting FWD (including progress to address any gaps)
- Progress of the annual compliance plan
- Key findings from risk assessments and compliance monitoring and testing
- Compliance incidents, breaches, issues and fines
- Regulatory actions or inspections
- Key compliance initiatives and projects
- Compliance training statistics (monthly only)

- Complaints analysis (quarterly reporting only)
- Whistleblower cases (quarterly reporting only)
- MI / Key Risk Indicators across key compliance risks (quarterly reporting only)

## 7. Outsourcing

As per the FWD Group Outsourcing Policy, the Compliance function should not be outsourced. However, should there be a decision to outsource any activities performed by the Compliance function, Group Compliance should have a degree of oversight, and accountability for any outsourced arrangements. Please refer to the FWD Group Outsourcing Policy for further information.

## 8. Review of this policy

This policy is subject to review at least every 2 years, or more frequent review to comply with the applicable changes to legislative and regulatory requirements.

## 9. Dispensation

Any deviation from this policy should be requested by Chief Compliance Officer for Group Chief Compliance Officer's dispensation. The written request of dispensation will only be considered where the request details the solid reasons for the use of alternative approaches will provide more prudent, robust and practical result of an assessment of the risk profile for the respective BU.

C2 - Internal



## FWD Life Insurance (Cambodia) PLC.

### Risk Appetite Framework

Document ID	KH-CG_RM-FW-0001	Document type	Framework
Issued by / Owner	Chief Legal and Compliance Officer	Approved by	Board of Directors
Target audience	All the staff and Directors of FWD		
Document status	In-Effect	Date Last Approved	27 <sup>th</sup> April 2022

#### Document approval history

Version	Date approved	Description
1.0	27 <sup>th</sup> April 2022	First version

# Contents

1. Purpose and Scope.....	3
2. Risk Appetite Framework .....	3
2.1. Risk Philosophy .....	4
2.2. Risk Appetite .....	4
2.3. Risk Metrics and Limits.....	7
3. Risk Appetite Governance.....	9
3.1. Roles and Responsibilities .....	9
3.2. Escalation Mechanism .....	11
4. Risk Appetite Reporting.....	12
5. Risk Appetite Communication and Review .....	12

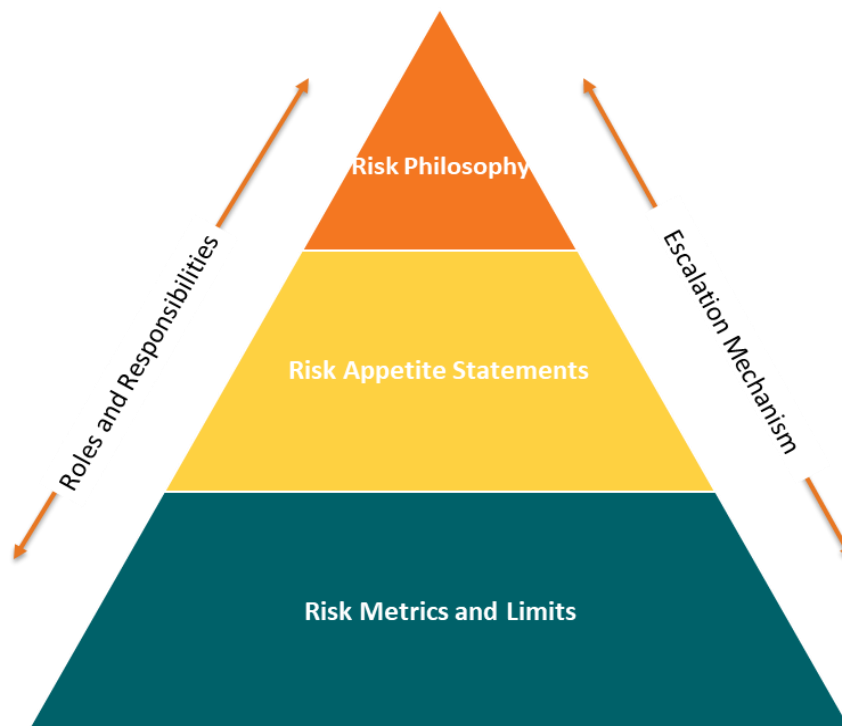


## 1. Purpose and Scope

FWD Life Insurance (Cambodia) PLC. (hereafter termed as “FWD” or “Company”) is a financial services company that provides wealth management and protection products to end consumers and is therefore exposed to a variety of risks. The Company has established a Risk Appetite Framework (“RAF”), described by this document, to define the Board of Director’s (“Board”) attitude to such risks and to guide the achievement of business objectives within the bounds of acceptable tolerances and limits.

## 2. Risk Appetite Framework

The RAF organises the Company’s overall approach to selecting the risks it wishes to seek, retain, transfer and/ or avoid in the pursuit of its strategic objectives and guides key business activities to operate within the bounds of the framework. The RAF is comprised of (a) Risk Philosophy, (b) Risk Appetite Statements and (c) Risk Metrics and Limits which are further supported by robust governance – roles, responsibilities and escalation mechanisms – as illustrated in the figure below.



The RAF forms a critical element of the Enterprise Risk Management Framework (“ERMF”) which organises FWD’s overall approach to risk management and supports the embedding of a strong risk culture. In return, a strong risk culture provides an environment that helps ensure any risk-taking activities beyond the Company’s risk appetite are recognised, escalated and addressed in a timely manner.

## 2.1. Risk Philosophy

FWD’s Risk Philosophy defines the overall attitude towards risk, with consideration to our vision, corporate strategy and the expectations of key stakeholders. The Risk Philosophy therefore demonstrates a critical linkage between FWD’s business objectives and its approach to risk management.

The company has articulated its risk philosophy as follows:

Risk Philosophy	<p>FWD’s vision is to “change the way people feel about insurance”, from which the Group’s business strategy and Risk Philosophy are derived. FWD aims to realise this vision through growth, simple and innovative products and relevant solutions, and best-in-class customer experiences. We focus on maintaining financial stability and creating long term sustainability through achieving scale and effective risk and capital management.</p> <p>In the pursue of our strategic objectives, we consider the interest of all stakeholders. FWD’s risk appetite seeks to manage the level of risk-return that enables FWD to meet the obligations to its policyholders, whilst creating long-term value for its shareholders.</p> <p>This Risk Philosophy forms an integrated part of the Risk Appetite Framework to inform the articulation of Risk Appetite Statements.</p>
-----------------	---

The Risk Philosophy is further expanded through underlying components of the RAF described below.

## 2.2. Risk Appetite

The Company has established Risk Appetite Statements (“RAS”) to determine the extent of risk that the Board is willing to accept within its risk capacity in the pursuit of its key business objectives (“Appetite Statement”) and to define the actions to be taken in order to remain within the risk appetite (“Actionable Statement”). The Appetite and Actionable Statement are defined for each material risk to which FWD is exposed in the pursue of its key business objectives.

The RAS should be:

- Comprised of qualitative and quantitative measures that take into consideration all relevant and material categories risks and their interdependencies within the Company’s current and target risk profiles; and
- Assessed against the business plan and a range of plausible future scenarios.

### 2.2.1. Key Business Objectives

The Company has expressed the key business objectives as follows:

Strategy	FWD aims to achieve its Company’s vision and strategic objectives, in particular from adoption of disruptive technologies, increasingly data-driven decision making and testing of innovative distribution channels to strengthen customers’ experience and enhance competitive advantage
Financial	FWD aims to manage its business to ensure it maintains sufficient capital for the Company to support the Minimum Capital Requirement and sufficient funding to support the business activities and capital needs of Company, whilst creating sustainable value and earnings consistent with stakeholder’s expectations.
Business Practices	In the pursue of its vision and strategic objectives, FWD aims to maintain its operational resilience and its commitments to customers and other external stakeholders, and to avoid material adverse impact on its reputation, thereby building long-term trust and demonstrating itself as a responsible firm amongst its key stakeholders and the local community within which the Company operates.

### 2.2.2. Risk Appetite Statements

Corresponding to each key business objective, the Company has expressed the risk appetite statements as follows:

Strategy:		
	Appetite Statement	Actionable Statement
Strategy Risk	<ul style="list-style-type: none"> <li>FWD accepts strategic risk as part of its business planning process and pursue of its vision and strategic objectives.</li> <li>FWD has no appetite for business activities or decisions that knowingly lead, or are likely to lead, to negative impacts on FWD’s brand value or customer outcome.</li> </ul>	<ul style="list-style-type: none"> <li>We adhere to our vision and continue employing technologies to innovate our distribution, products and services that enable the improvement in customer experiences.</li> <li>In the implementation of our growth strategy, we use a balanced approach to risks and controls that employs sound risk management principles, whilst considering the interest of all stakeholders.</li> <li>FWD continues to monitor internal and external events that can negatively influence stakeholders’ perception of its strategy or can adversely impact FWD’s brand value or customer outcome.</li> </ul>

Financial:		
	Appetite Statement	Actionable Statement
Market Risk	<ul style="list-style-type: none"> <li>FWD accepts market risk exposure where it has ample understanding and is able to manage its position as a long-term investor to generate adequate and sustainable risk-adjusted returns for the benefit of its policyholders and shareholders.</li> <li>FWD has no appetite for complex market risks for which the Company has no knowledge.</li> </ul>	<ul style="list-style-type: none"> <li>To mitigate excessive exposures to market risks, FWD ensures effective asset-liability management, including prudent use of derivatives for risk management purposes, and to mitigate excessive exposures.</li> <li>FWD does not speculate in foreign exchange exposures. Where exposures arise as part of business activities, the risk should be hedged (or otherwise) as deemed appropriate.</li> </ul>
Credit Risk	<ul style="list-style-type: none"> <li>FWD has a low appetite for credit risk arising from a default by an insurance, reinsurance or investment counterparty (except for credit investments) to fulfil its obligations to the Company.</li> </ul>	<ul style="list-style-type: none"> <li>To mitigate the exposure to credit risk, FWD seeks to engage in transactions with highly-rated counterparties.</li> </ul>
Insurance Risk	<ul style="list-style-type: none"> <li>FWD accepts insurance risk exposure that the Company has the experience to understand, ability to measure and reasonable expectation to price and derive value for shareholders and customers.</li> </ul>	<ul style="list-style-type: none"> <li>To reduce excessive exposure to insurance risk (e.g. in the absence of relevant experience and knowledge), FWD makes use of reinsurance or other forms of risk transfer when deemed necessary.</li> <li>FWD seeks to ensure that insurance risk acceptance and valuations are based upon robust operating assumptions to reduce risk of deviation in actual experience, and reviews the operating assumptions regularly.</li> </ul>
Liquidity Risk	<ul style="list-style-type: none"> <li>FWD has a low appetite for liquidity risk arising from operating expenses and dividends.</li> </ul>	<ul style="list-style-type: none"> <li>FWD ensures that sufficient financial resources are available to meet the financial obligations.</li> </ul>

Business Practices:		
	Appetite Statement	Actionable Statement
Legal, Compliance & Reputational Risk	<ul style="list-style-type: none"> <li>FWD accepts operational risk is an inherent part of business operations and has varying appetite and tolerance levels for different types of operational risk.</li> <li>FWD has no appetite for behaviours and decisions that knowingly lead, or are likely to lead, to unfair customer outcomes, regulatory intervention, breach of code of conduct or reputational damage.</li> <li>FWD has low appetite for adverse business resilience and no appetite for control deficiencies that result in material losses (direct or indirect).</li> </ul>	<ul style="list-style-type: none"> <li>To remain within the risk appetite, FWD escalates any high or extreme operational risk events to the Audit Committee and Board, which requires immediate mitigation actions.</li> <li>FWD will always act with good faith and intention for fair customer outcome and regulatory compliance, and requires its employees and third parties to adhere to its Code of Ethics and Business Conduct.</li> <li>FWD has a robust and effective risk-based control environment to mitigate the risk of unfair customer outcome and adverse business resilience, while minimising financial losses arising from operational failures and control deficiencies.</li> </ul>

## 2.3. Risk Metrics and Limits

### 2.3.1. Risk Metrics

Risk Metrics and Limits provide the capability for FWD to measure its actual exposures relative to the RAS, evaluate the extent to which day-to-day business activities are within the bounds of risk appetite and determine whether any mitigation action is required.

In setting Risk Metrics and Limits, FWD considers its preferences for each risk factor in addition to historical data, regulatory expectations, industry practices, expert judgment and other considerations where available and relevant to quantify the maximum level of risk desired. For certain risk factors where quantification is not possible (e.g., non-financial risk), the company adopts a qualitative approach based on the FWD risk assessment methodology and risk level matrix<sup>1</sup>.

Aligned to each key business objective, the company has defined its Risk Metrics as follows. Thresholds are set to determine the extent to which actual exposures are within the bounds of overall risk appetite.

Key Business Objective	Risk Metric	Low	Medium	High	Extreme
Strategy	VONB growth against plan	Above 90% of Plan	70%-90% of plan	Below 70% of plan	N/A
Financial	Regulatory Capital level	Solvency Margin at least 120%	Solvency Margin at least 110% but less than 120%	Solvency Margin at least 100% but less than 110%	Solvency Margin below 100%
Business Practices	FWD Reputation and Regulatory Intervention	No negative media attention and no regulatory intervention	Negative media report but low customer impact or minor breach of regulation or law (leading to minor regulatory action)	Sporadic negative media exposure or multiple related minor breaches or single serious breaches resulting in regulatory enforcement action	Prolonged negative media exposure leading to loss of public confidence and reputation or significant regulatory enforcement action and intervention

### 2.3.2. Key Risk Indicators

For each risk appetite statement defined in section 2.2.2, Key Risk Indicators (“KRIs”) are developed to monitor whether the company is operating within the defined risk tolerance. The below table provides an overview of the KRIs and thresholds.

Key Business Objective	Key Risk Indicators	Low	Medium	High	Extreme
Strategy	Total Weighted Premium Income (TWPI)	Above 90% of Plan	70%-90% of plan	Below 70% of plan	N/A
Financial	Operating Expense Overrun (to Plan)	<= 100%	100.1% - 130%	>130%	N/A
Business Practices	Business interruptions	Business interruption for less than 4 hours.	Business interruption for 4 to 24 hours.	Short term cessation of core activities from 24 to 48 hours. Adversely affects a key business stakeholder.	Cessation of activities from 48 hours to one week. Adversely affects multiple key business stakeholders.

## 3. Risk Appetite Governance

### 3.1. Roles and Responsibilities

Whilst ownership of the RAF resides with the Group Board, its effective operation is contingent upon the contribution and involvement of stakeholders across FWD. Key roles and responsibilities are outlined in the sections below.

#### 3.1.1. Board

The Board is ultimately accountable for establishing and overseeing an effective ERMF, including the RAF. To fulfil this responsibility, the Board should:

- Approve the overall RAF, Risk Philosophy and RAS on at least an annual basis, or in response to a material change in the business or risk environment;
- Approve mitigation actions and responses to breaches of RAS;
- Ensure that the RAF has been effectively communicated to appropriate stakeholders (internal and external) and integrated in key business decision-making;
- Ensure that a strong risk culture is promoted and embedded throughout the business operation to support implementation of the RAF; and

#### 3.1.2. Audit Committee

The Audit Committee (“AC”) is delegated authority by the Group Board to implement the ERMF and RAF. To fulfil this responsibility, the AC should:

- Approve mitigation actions and responses to breaches of Risk Metrics, also reviewing proposed business activities which may deviate from risk appetite prior to submission to the Board;
- Review the overall RAF, Risk Philosophy and RAS on at least an annual basis and recommend to the Board for approval as appropriate; and
- Support communication of the RAF to appropriate stakeholders (internal and external) and promote the integration of risk appetite in key business decision-making.

#### 3.1.3. Executive

The Executive – either in their individual capacity or as part of the Executive/ Management Committee (“ExCom”) or other senior management committee – is responsible for ensuring that activities of their respective business functions are carried out in alignment with the RAF. To fulfil this responsibility, the Executive should:

- Approve the implementation of robust internal controls, or completion of other remedial actions, to address risk appetite breaches or other deficiencies raised by Risk Management, Compliance or Audit;
- Review the overall RAF, Risk Philosophy and RAS to provide feedback for consideration by the Risk function;
- Propose appropriate mitigation actions in response to a breach of RAS;
- Propose Risk Metrics, Key Risk Indicators and corresponding limits to enable effective measurement of risk exposures in collaboration with Risk Management, Compliance and other relevant parties;

- Ensure that day-to-day activities of their respective functions are undertaken with consideration to the RAF, including RAS, Risk Metrics and KRIs as relevant; and

### 3.1.4. First Line of Defence Functions

First Line of Defence Functions are tasked with carrying out day-to-day activities in accordance with the approved RAF (and broader aspects of the ERMF). To fulfil this responsibility, staff should:

- Develop robust internal controls, or undertake other remedial actions, to address risk appetite breaches or other deficiencies raised by Risk Management or Audit;
- Develop appropriate mitigation actions in response to a breach of RAS, Risk Metrics and KRIs in collaboration with Risk Management, Compliance and other relevant parties ; and
- Support the Risk function, as required, to design and implement the overall Group RAF, Risk Philosophy and RAS – including provision of data regarding Risk Metrics and KRIs.

### 3.1.5. Head of Risk (or equivalent)

The Head of Risk (or equivalent) is responsible for the overall design of the RAF. In particular, the Head of Risk should:

- Review actual exposures relative to risk appetite, including identification of breaches (actual and anticipated) and review of mitigation actions proposed by the Executive;
- Review the Risk Metrics, KRIs and corresponding limits proposed by the Executive to their submission to the AC;
- Propose the overall RAF, Risk Philosophy and RAS on at least an annual basis for consideration by the AC and the Board;
- Propose changes to the RAF in response to a material change in the business or risk environment for submission to the AC and the Board ;
- Communicate the RAF to appropriate stakeholders (internal and external) and ensure the integration of risk appetite in key business decision-making and adequacy of risk reporting; and
- Document the RAF, including RAS, Risk Metrics and KRIs, as part of this document (and other related documents) in alignment to internal and external (e.g. regulatory) expectations.

### 3.1.6. Risk Management (Second Line of Defence)

The Risk function should:

- Develop the overall, Risk Philosophy and RAS and review on at least an annual basis for consideration by the AC and the Board ;
- Develop and maintain capabilities to monitor and report actual exposures relative to risk appetite, including identification of breaches (actual and anticipated) and review of mitigation actions;
- Identify changes required to the RAF in response to a material change in the business or risk environment;
- Document the RAF, including RAS, Risk Metrics and KRIs, as part of this document (and other related documents) in alignment to internal and external (e.g. regulatory) expectations.



- Support the Executive and First Line of Defence functions, as required, to integrate risk appetite in key business decision-making.

### 3.1.7. Internal Audit (Third Line of Defence)

Internal Audit is responsible for performing an independent assessment of the ERMF, including the RAF, and raising any findings and recommendations to Executive Management.

Internal Audit may report matters directly to the Audit Committee.

## 3.2. Escalation Mechanism

The Enterprise Risk Management Policy defines the risk management escalation process, including four tiers – “Low”, “Medium”, “High” and “Extreme” – to ensure matters are visible to and managed by stakeholders with appropriate authority and understanding to decide upon the Company’s response. For the purposes of the RAF, responsibility resides with the following for approval of risk acceptance and remedial actions where breaches occur.

Risk Component	Low	Medium	High	Extreme
RAS Risk Metrics	No escalation, routine monitoring and reporting.	Line risk manager to act, immediately upon identification. Action at risk owner discretion.	Group Risk and Audit Committee escalation, immediately upon identification. Immediate actions to be developed.	Group Risk and Board escalation, immediately upon identification. Immediate actions to be developed.
Key Risk Indicators	No escalation, routine monitoring and reporting.	Line risk manager to act, immediately upon identification. Action at risk owner discretion.	Audit Committee escalation, immediately upon identification. Immediate actions to be developed.	Group Risk and Board escalation, immediately upon identification. Immediate actions to be developed.

Note: any instances whereby immediate escalation is required should be raised to the Group CRO who will notify the relevant stakeholder(s) through an appropriate means (e.g. email or convening a special meeting of the committee).

## 4. Risk Appetite Reporting

Risk Function are responsible for reporting, on at least a quarterly basis, exposures against Risk Limits to the Group Risk Function and may provide reporting to the Senior Management Team and relevant committees as required.

Any violation or anticipated breach of risk appetite should be immediately escalated to the Senior Management Team and reported to the Group CRO who will further escalate the matter to relevant stakeholders in accordance with the escalation criteria outlined in section 3.2.

## 5. Risk Appetite Communication and Review

Following approval of the RAF, the risk appetite should be communicated internally to relevant stakeholders to ensure the statements, limits and other components remain transparent and visible throughout the Company. At a minimum, the communication should extend to those stakeholders outlined under section 3.1 to ensure that all relevant staff are aware of and have the competence to discharge their duties in accordance with the RAF.

In addition, risk appetite may be communicated externally to our regulators, investors and policyholders – for example through inclusion in the annual financial disclosures and report.

The Company's RAF is subject to review on at least an annual basis, or more frequently in response to a material change in the business, risk or operating environment (i.e. an "ad-hoc" review). Such review serves to ensure that the RAF remains appropriate for the nature, scale and complexity of the FWD's operations and business strategy. Further, the RAF should be independently assessed by internal audit or independent external parties at least once every three years as part of a review of the ERMF.

- End of Document -

C2 - Internal



## FWD Life Insurance (Cambodia) PLC.

### Enterprise Risk Management Framework

Document ID	KH-CG_RM-FW-0002	Document type	Framework
Issued by / Owner	Chief Legal and Compliance Officer	Approved by	Board of Directors
Target audience	All Directors, management, employees and contractors at all levels		
Document status	In-Effect	Date Last Approved	27 <sup>th</sup> April 2022

#### Document approval history

Version	Date approved	Description
1.0	27 <sup>th</sup> April 2022	First version

# Contents

1.	Purpose & Scope .....	3
2.	Enterprise Risk Management Framework and Compliance Principles .....	3
3.	Risk Governance .....	4
3.1	Risk Governance Structure .....	5
3.2	Three lines of Defence .....	5
3.3	Roles and Responsibilities.....	6
4.	Risk Culture and Key Performance Indicator .....	7
4.1	Risk Culture .....	7
4.2	Risk and Compliance KPI.....	8
5.	Risk Appetite Framework .....	8
6.	Risk Classification .....	9
7.	Risk Management Process .....	10
7.1	Risk Identification .....	10
7.2	Risk Assessment .....	11
7.3	Risk Response.....	11
7.4	Risk Monitoring and Review .....	12
7.5	Communication and Improvement .....	13
8.	Risk Assessment Methodology .....	13
8.1	Likelihood .....	14
8.2	Impact .....	14
8.3	Risk Level.....	18

## 1. Purpose & Scope

FWD Life Insurance (Cambodia) PLC. (hereafter termed as “FWD” or “Company”) is a financial services company that provides wealth management and protection products to end consumers and is therefore exposed to a variety of risks.

This document describes the framework (“Framework”) necessary to identify and manage risks at FWD. The Framework is approved by the Board and is supportive to the business objectives and strategies on all levels.

**Purpose** This Framework covers establishing the risk appetite, which is an expression of the level of risk FWD is prepared to take to achieve its strategic objectives. The Framework establishes the risks FWD wishes to acquire, avoid, retain and/or remove in pursuit of its strategic objectives.

This Framework provides a common language and clear roles and responsibilities in setting and managing our risk appetite across risks FWD is exposed to including, strategic, insurance, operational and compliance, and investment, ALM and capital market risks. All functional areas in the businesses of the Company are in scope.

**Review** This Framework should be reviewed at least annually to ensure continued appropriateness to FWD. The review is to be conducted by the Head of Risk and Head of Compliance (or equivalents), and any material changes require approval by the Board.

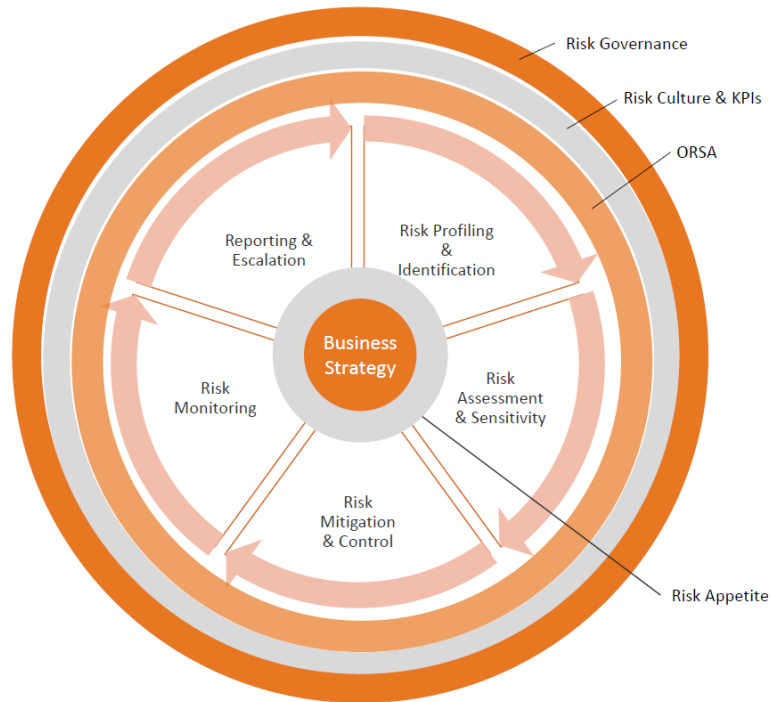
The effectiveness of the ERM Framework is required to be regularly reviewed to ascertain that the ERM Framework remains fit for purpose. A feedback loop is required to make necessary and timely remedial actions or improvements to the ERM Framework.

Independent review of the ERM framework is required once per every three years, which should be carried out by suitably experienced individual(s) who reports directly to the Board.

**Dispensation** Any deviation from this Framework are required to submit a written request for dispensation from Group CRO (and Group Chief Compliance Officer for compliance related requirements). Dispensation will only be granted if there is strong justification to support that alternate arrangements are more robust than this framework and more appropriate for the company’s circumstances.

## 2. Enterprise Risk Management Framework and Compliance Principles

FWD must implement the enterprise risk management and adopt the compliance principles consistent with this Framework shown in the graph.



### Compliance Principles

Our business activities are highly regulated to varying degrees across the markets within which we operate, exposing us to a variety of inherent compliance risks. To minimise and manage these compliance risks, FWD is committed to the design and progressive implementation of a risk-based compliance management process across all of our businesses. At FWD, the compliance management process is part of the wider ERM Framework.

In line with our Code of Ethics and Business Conduct, we believe in “Doing the Right Things Right”. Compliance at its most fundamental level is simply about “Doing the Right Things Right”. Therefore, our approach to Compliance is primarily concerned with the quality of our practices and processes. It is about ensuring that everyone at FWD knows, or knows how to easily find out, what is the right thing to do every day in every aspect of their role, all playing a part in managing compliance risks.

## 3. Risk Governance

The Board has the overall responsibility to establish and oversee an effective ERM Framework, while all management and staff in the Company are responsible for risk management. FWD’s risk governance is based on the “**three lines of defence**” model which ensures that risk is managed within the risk appetite as approved by the Board and cascaded throughout the Company.

### 3.1 Risk Governance Structure

The Board established a Audit Committee (or “AC”) that advises the Board on effective and efficient management of the Company’s business operations. In term of risk management, AC is responsible for the company’s risk appetite, key risk management and compliance policies and procedures, and in reviewing the adequacy and effectiveness of the ERM Framework.

In terms of control functions, Risk Management and local Compliance functions, which report directly to the Group Risk Management and Group Compliance functions, coordinate risk and compliance management activities in the functional units of the Company. Risk Management and Compliance function also report to local management and the AC.

### 3.2 Three lines of Defence

The Three Lines of Defence Model distinguishes among 3 groups involved in effective risk management: 1. Functions that own and manage risks; 2. Functions that oversees risks; and 3. Functions that provide independent assurance.

#### 1st Line of Defence

The Business itself, management and employees who take and manage risk day to day in accordance with the strategies, this framework and risk appetite set by the Board along with policies and standard operating procedures. The first line of defence develops and implements mitigation activities including monitoring and reporting for managing risk and ensuring compliance with all legal and regulatory requirements in business activities.

#### 2nd Line of Defence

The Risk Management and Compliance functions:

- support and assist the Board, senior management and the relevant risk committees to formulate the firm’s appetite for risk, risk management and compliance strategies, policies and limit structures;
- coordinate, oversee and objectively challenge the execution, management, control and reporting of risks;
- provide second opinion on the risk exposures; and
- provide oversight, monitoring and assessment as to the effectiveness of the ERM Framework.

#### 3rd Line of Defence

The Audit Committee, provides independent assurance on the design and effectiveness of the overall system of internal control, including Risk Management, Legal and Compliance.

### 3.3 Roles and Responsibilities

The key roles and responsibilities with respect to enterprise risk management are shown below.

- |  |   |
|--|---|
| <b>Board</b>                                       | <ul style="list-style-type: none"> <li>• Has overall responsibility for establishing and overseeing an effective ERM Framework</li> <li>• Establishes an organizational structure for risk management</li> <li>• Sets up and embrace a sound risk and compliance culture and effective risk and compliance management practices</li> <li>• Approves the Code of Ethics and Business Conduct</li> </ul>  |
| <b>Audit Committee<br/>(risk management roles)</b> | <ul style="list-style-type: none"> <li>• Is set up by the Board</li> <li>• Provides advice to the Board relating to risk appetite, risk and compliance management frameworks</li> <li>• Monitors the risks associated with the implementation of the Company's strategies</li> </ul>  |
| <b>1<sup>st</sup> Line Management</b>              | <ul style="list-style-type: none"> <li>• Is responsible for effective internal controls and risk management</li> <li>• Is responsible for ensuring compliance with regulatory obligations</li> <li>• Monitors and evaluates the overall risk profile to ensure that FWD operates to achieve its business objectives within the relevant risk appetite and tolerance.</li> </ul>   |
| <b>Compliance (and Risk Management) Function</b>   | <ul style="list-style-type: none"> <li>• Facilitate a risk culture that embed the consideration of risks taken business decisions. When prevention fails, facilitates the speedy detection of the issue and ensures rectification quickly and effectively as part of a continuous improvement process.</li> <li>• Facilitates functional units in managing their business risks and coordinating risk management activities across the Organisation.</li> <li>• Identifies all applicable Compliance requirements for the company and the risks involved</li> </ul> |



- Effectively mitigates compliance risks by engaging the business at all levels and ensures employees know how to do the right things right by translating compliance requirements into policies, procedures, training and controls.
- Supports a culture of integrity and trust which encourages active participation by employees to speak up and report compliance issues or concerns.
- Monitors the effectiveness and efficiency of compliance procedures controls, and arrangements.
- Facilitates strong, effective and trusting relationships with regulators and the industry
- Provide objective challenge and support and escalate matters when necessary to help optimize the trade-off between risk and reward.
- Provides support and opinion to the Board, Audit Committee and 1st Line Management to establish and implement appropriate policies and procedures in relation to the ERM Framework.

## 4. Risk Culture and Key Performance Indicator

FWD aims to build a strong risk culture across the Company where the Risk and Compliance Key Performance Indicators (“RCKPI”) are set up to encourage and steer its development.



### 4.1 Risk Culture

Risk culture is the set of shared values and behaviours of all staff in FWD that influence risk decisions. FWD aims to maintain a risk culture which enables proactive management of risk by all staff across the organisation. The Guiding Principles in the Code of Ethics and Business Conduct set out the behavioral standards expected of every director, officer, employee, agent and contractor as part of their employment or appointment with FWD.

At FWD, we believe that the “tone from the top”, leadership engagement, accountabilities and awareness and communication initiatives are key to ensure that a strong risk culture is prevalent across the organisation. A visible focus on risk at the highest level of management emphasises the importance of and encourages risk awareness. This is demonstrated through FWD’s commitment toward the three lines of defence risk governance model and the Executive Committee’s participation in the risk committees. Tools including survey will be applied in measuring the effectiveness of FWD’s risk culture. An improvement plan on risk culture should be established on annual basis.

## 4.2 Risk and Compliance KPI

Risk and Compliance Key Performance Indicator (RCKPI) must be set up annually to encourage all staff to demonstrate proper behaviours (e.g. adhering to business policies, timely notification of incidents or issues when they become aware, etc.) and to manage risk within the approved tolerance and escalating issues accordingly. Risk Management and Compliance functions are responsible to provide a self-assessment including all things that have gone well and also areas for improvement to Group Risk Management and Group Compliance at least by quarterly basis. The annual calculation design and final results of the RCKPI should be recommended by Group CEO based on proposal from Group Chief Risk officer and Group Chief Compliance Officer, and they should be approved by Group Risk Committee and Group Compensation Committee.

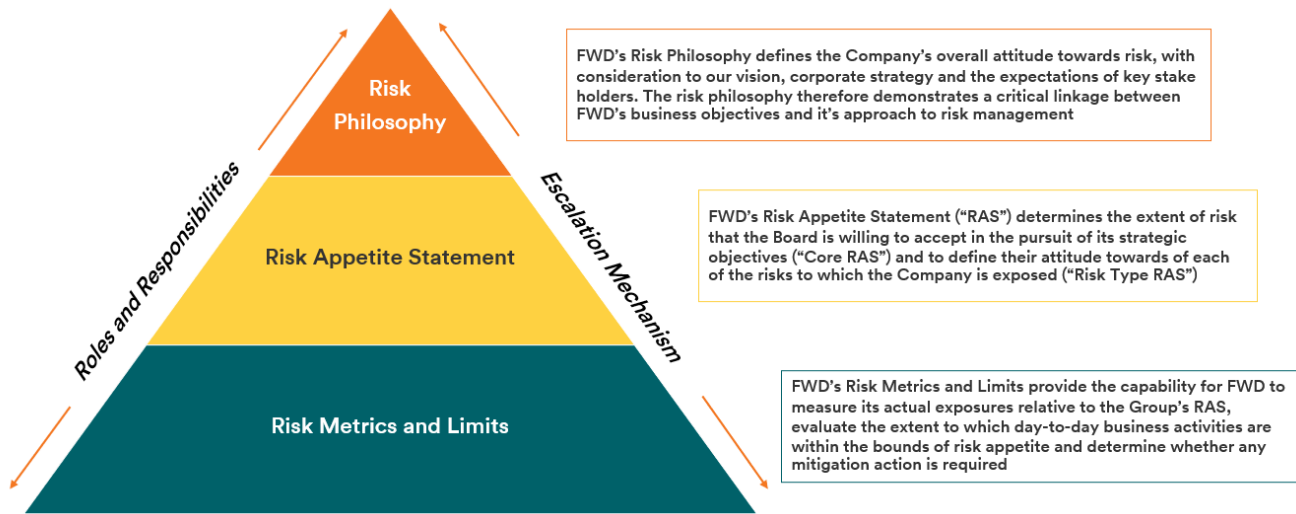
## 5. Risk Appetite Framework

When managing risk it is important to have a common language that links our view and appetite for risk with the strategic objectives of our company. To this end, the Risk Appetite Framework is defined as:

- the risks that FWD wishes to acquire, avoid, retain and/or remove in its pursuit of its strategic objectives.
- Consists of risk preferences, risk tolerances, risk limits and controls which are linked to FWD's strategic objectives.

The Board is responsible for approval of the Risk Appetite Statement ("RAS"). Executive Committees ("ExCom") and Functional Heads should cascade down more detailed interpretations and implementations of the risk appetite, and ensure the RAS is communicated to and understood by internal and external stakeholders. They should monitor and control their activities and business transactions to ensure that it's in line with the risk appetite.

Risk appetite links the annual planning process, which set business targets in line with the Company's strategic objectives, with the quarterly enterprise risk management cycle in which the Company's management analyses the risks and take risk mitigating actions to manage the risk within the risk appetite. It is crucial that the risk appetite is reviewed as part of the annual planning cycle connecting strategic, financial, operational and capital objectives with the risk appetite. The ultimate objective is to ensure an optimum risk adjusted return on capital for risk taking that aligns with the Company's overall risk preferences and strategic objectives.



## 6. Risk Classification

To systematically assess and manage risks across the Group, risks have been classified into four categories as detailed below. These categories can be broken down further to sub-categories which is described in detail in the ERM Policy. The relevant risk committee is responsible for reviewing and approving the appropriate supporting policies as well as overseeing compliance with those policies.

### Strategic Risks



This covers corporate level issues FWD faces, particularly those related to the competitiveness and sustainability of FWD.

Strategic risks also address issues that involve the long term direction of FWD and the contagion risk for the Company.

### Insurance Risks



Many insurance related risk parameters are characterized by the following three risk components.

- Volatility - the risk that actual value differs from expected, assuming the best-estimate parameter is true. Volatility is the result of the randomness of the risk process.
- Calamity - the risk of a one-time claim of extreme proportions due to a certain major event, which is not caused by a change of the parameters. The event can be viewed as a one-year shock. Examples of calamity risk are epidemics, earthquakes, big flood, terrorist attack, etc.
- Uncertainty - the risk of parameter estimation as a result of statistical estimation errors and changes of parameter over time.

**Operational  
and  
Compliance  
Risks**



The risk of loss resulting from inadequate or failure in internal processes, people and systems or from external events is defined as operational risk, including compliance and legal risk.

Compliance risk considers losses from damage to reputation, legal or regulatory sanctions, financial loss or loss of license to operate which flow from failure or perceived failure to meet the Company’s compliance obligations.

**Investment,  
ALM and  
Capital risks**



Collectively known as financial risks these cover risk arising from direct investments, or exposure to credit or investment market risk, including macro-economic risks that for example determine long-term interest rates. Capital risk arise from the strategic, or tactical allocation of capital/assets and the inherent balance sheet exposure this creates, but also investment performance risks.

These are among the principal risks of an insurance company and key drivers of capital requirements.

## 7. Risk Management Process

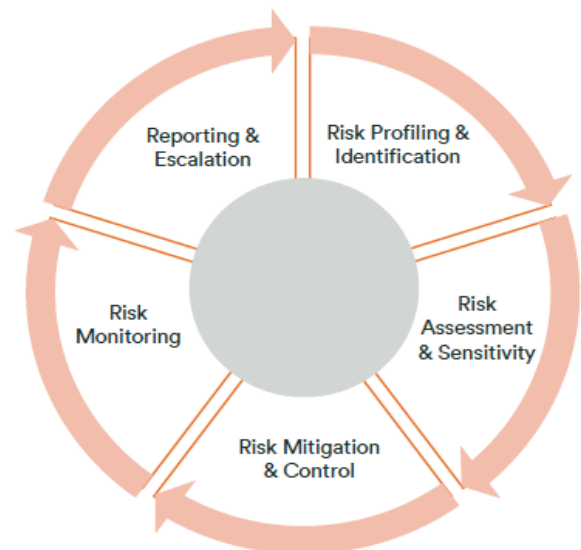
FWD operates in the insurance sector, so it is in the business of taking and managing risks. It is therefore needed to ensure that FWD has a robust adaptive control cycle risk management in place to: identify risk; assess the risk; manage the risk; monitor; and communicate.

### 7.1 Risk Identification

Risk identification is the identification of uncertain issues or factors that determine the success or failure of a business unit or a business process. The ability to identify risks systematically and comprehensively ensures that extreme or high risks are not unwittingly excluded.

Risk identification involves consideration of the following:

- business objectives;
- critical success factors;
- issues that would affect the achievement of the objectives;



- experiences from the past in dealing with issues and problems in the area;
- analysis of potential scenarios that could happen to the area; and
- intra-group transactions.

## 7.2 Risk Assessment

The Risk Level shall be assessed for the following 3 stages:

**Inherent risk:** Assessment of risks assuming that no controls exist.

Assessment of inherent risk is recommended as it gives a good understanding of the gross exposure to the activity, and shall be based on incident data (scenario) analyses;



**Managed risk:** Assessment of the risks in their current control environment. Assessment of managed risk requires the identification of all relevant existing controls and the assessment of the control's effectiveness. Analysis/evaluation of the difference between the inherent and managed risk can provide a good understanding of effectiveness of the existing controls;

**Residual risk:** Assessment of the risks in their current control environment and future mitigation actions. For each possible future mitigation action a cost/benefit analysis shall be performed. Extreme and High managed risks should be escalated to the Group Office to determine how they are to be managed. Moderate risks are tolerated and can be accepted. Low risk is acceptable risk.

Risks are assessed in two dimensions – likelihood and impact, and then be classified into the one of the four risk levels of (Extreme, High, Moderate or Low). The detailed guide to assessment of likelihood and impact is in section 8 Risk Assessment Methodology.

## 7.3 Risk Response

Based on the results of the risk assessment, prompt response measures must be determined for the risks which were assessed at an Extreme or High risk level. Risk response actions are determined based on the expected cost for implementing these options and the expected benefits from these options (e.g. change in risk likelihood and impact). When large reductions in risk may be obtained with relatively low expenditure, such options should be implemented.

Both the upside and downside risks should be considered and if the upside opportunity outweighs the downside loss then a decision should usually be made to proceed with the action or initiative.

The risk assessment process results in a risk assessment report which reflects all (managed and residual) risks and controls. Management and/or the Board can formally accept the residual risks and decide which of the preferred response measures will be put in an action plan for implementation with a clear assignment of the required actions (Person-To-Act), including time schedules (Due Dates).

The response measures and action tracking will be done by the relevant committees. Residual risks that exceed the approved risk appetite must be escalated to the Risk Management Committee if deemed necessary. In general this is the case for all Extreme and High managed or residual risks.

Risk response can be achieved through one or combinations of the following mitigation strategies: 1. reduce likelihood, 2. reduce impact, 3. avoid, 4. transfer and 5. accept. Acceptance of a risk beyond appetite (i.e. managed and/or residual risk level rated as Extreme or High) or beyond any risk limits must be escalated by the risk owner to the relevant risk committee(s) or Boards for approval.



## 7.4 Risk Monitoring and Review

Monitoring is assessing whether FWD is in control of its risks. Monitoring is a continuous process to measure and evaluate the effectiveness of the internal controls and to determine whether the risks are within the norms for risk appetite and in line with the desired levels and whether policies, minimum standards and regulations are adhered to.

Monitoring can be performed through various techniques supported by automated or other tools. Examples include management reports, monitoring of risk indicators, action tracking, key control testing, supervision, quality assurance, back-testing, policy review or self-assessment. Common features of all monitoring activities are that they:

- are used to validate a situation, statement or assumption (risk or control statement);
- have a sound basis (evidence);
- are well documented; and
- lead to conclusion on the (risk) controls.

Both the design effectiveness of a control and the operating effectiveness are subject to monitoring and different techniques may be used. Monitoring of the design effectiveness should safeguard that for each risk, controls are defined and that the design is effective. The basis for the design effectiveness is an updated risk analysis for the process/system/organisation involved. Through monitoring by measurement and testing the continuous effective operating of the control can be ensured.

Through quality assurance and control, Compliance & Risk Functions assess the monitoring embedded in the Functional Units. Quality assurance and control is performed through reviews of required test documentation. Risk Functions evaluate whether the risk response is still in line with the risk appetite of the business and takes into account the risk profile that changes over time.

## 7.5 Communication and Improvement

Risk information has to be gathered, analyzed and communicated in a structured way to ensure the relevant personnel in FWD are aware of the risks and take responsibility for managing risk.

A risk awareness culture, being awareness of threats, risks and resilience at all levels, should be built by improving understanding, communication and education. Management, employees, contractors and third party users must be aware of information security threats and concerns, their responsibilities and liabilities. In addition, these individuals should be equipped to support FWD (information) security policies in the course of their normal works, and to reduce the risk of human error.

In order to meet the expectations and requirements for a sound risk awareness culture, FWD shall perform awareness campaigns, targeted at all personnel across the Company, by communicating and educating them about the risks involved in their daily works and the knowledge of how to address them seriously.

Appropriate communication channels should be established such that relevant personnel understand and adhere to the risk-related policies and procedures.

## 8. Risk Assessment Methodology

The ultimate goal of risk management is to assist the Company to optimize returns given the appetite for risk. Risk can be thought of as the chance of an unfavourable outcome compared with expectations



The expected outcome on average should be a favourable gain, however it is important to understand the risk of an unfavourable outcome. FWD’s methodology to assess this “tail risk” is described in the sections below.

## 8.1 Likelihood

Assessing the Likelihood dimension of risk involves considering how frequently the incident or event may occur over a specified time horizon. The typical Likelihood scale is characterized by 5 qualitative descriptive scales. For the purpose of risk consolidation, the scale can be translated into equivalent quantitative scale as shown in the table;

Level	Descriptor	Qualitative Description	Quantitative Description
A	Almost Certain	Is expected in most circumstances	Expected* to occur at least once a month
B	Likely	Will probably occur in most circumstances	Expected* to occur once every quarter
C	Possible	Might occur at some time	Expected* to occur once every year
D	Unlikely	Could occur at some time	Expected* to occur once every 5 years
E	Rare	May occur in exceptional circumstances	Expected* to occur less than once every 5 years

\* Expected to occur within the specified time horizon with a high (e.g. 95%) probability

## 8.2 Impact

It is important to recognize that the consequences of any particular risk event may impact in different ways: financial costs; personal harm (physical and psychological); legal consequences; and damage to reputation may all result from a single incident.

Quantitative impact is an assessment of the magnitude of gain (positive) or loss (negative) due to the occurrence of risk, covering both direct and indirect impact. This should be done at the 95% percentile level, however for the more material risks it is also informative to look at the maximum possible.

The table shows examples and guidelines of both Qualitative and Quantitative descriptors that may be assigned in relation to specific categories and impacts as may relate to a particular risk event. The impact should also consider emerging circumstances of the event and potential implications to FWD reputation and other stakeholders’ interests. Similar to likelihood, it is given a level of grading but this time in numerical form. E.g. if an accident will lead to death, it may be described as catastrophic and



graded level 5. Where an Impact falls into more than one category, the more serious impact should be used for calculation of risk level.

### Qualitative and Quantitative Measures of Impact of the Identified Assets

IMPACT Rating	Financial Loss (including compensation to customers)	Regulatory and Internal Governance	Operations	People	Reputation / Media Attention	Customer and Conduct	Asset Protection Security and safety of facilities
Insignificant Level 1	Direct loss or increased cost of up to USD10,000	N/A	Business interruption for less than 4 hours.	Isolated reduced employee morale and dissatisfaction Injuries requiring medical treatment leading to no lost workdays	Negative media report- low customer impact	Customers not aware of problem. Low customer impact < 5 customers	No damage or loss of FWD physical assets, facilities or property
Minor Level 2	Direct loss or increased cost of up to USD20,000	Minor and non-systematic breach of regulation or law not requiring mandatory reporting to the regulator and leading to minor regulatory action (e.g. request to enhance controls) Unintentional breach of internal governance document	Business interruption for 4 to 24 hours.	General reduced employee morale and dissatisfaction. Increase in employee turnover. Injuries requiring medical treatment leading to minimal workdays lost	Sporadic negative media exposure no regulatory impact. Short term damage to public confidence and reputation. Concerns of performance raised by shareholders, political or the community.	Some customers aware of problem. Affects 5 - 20 customers requiring redress or correction. Increase in customer complaints.	Minimal damage or loss of FWD physical assets or property. Minimal impact to facility or property security. Impact is limited to single facility / site and / or business / economic stakeholder
Moderate Level 3	Direct loss or increased cost of up to USD50,000	Multiple related minor breaches not requiring mandatory reporting to the regulator. Regulatory action possible but not published by regulator. Multiple related unintentional breaches of internal governance document.	Short term cessation of core activities from 24 to 48 hours. Adversely affects a key business stakeholder.	Widespread reduced employee morale and dissatisfaction. High turnover of experienced employees. Serious injuries requiring hospitalisation.	Regular negative media exposure requiring discussion with the regulator. Mid-term damage to public confidence and reputation. Serious decrease in shareholder, political or community support.	Significant number of customers aware of problems and encounter some inconvenience. Affects 21 -50 customers requiring redress or correction. Vulnerable customers as defined by regulations or internal policies/standards are affected.	Moderate damage or loss of FWD physical assets or property Moderate impact to facility or property security Impact to multiple facilities / sites and / or business / economic stakeholders
Major Level 4	Direct loss or increased cost of up to USD100,000	One or more serious breaches resulting in regulatory enforcement action (e.g. public reprimand by regulator, material fines levied or increased regulatory monitoring and reporting) Intentional breach of internal governance document.	Cessation of activities from 48 hours to one week. Adversely affects multiple key business stakeholders.	Significant turnover of experienced employees. Company not perceived as an employer of choice. Serious injury involving corporate negligence or loss of life.	Extended negative media exposure for e.g. investigative reporting likely to prompt regulator contact. Long term damage to public confidence and reputation. Significant loss of shareholder, political or community support.	Affects 51 - 100 customers requiring redress or correction. A breach of regulatory or legal compliance affecting > 20 customers)	Major damage or loss of FWD physical assets or property Major impact to facility or property security Widespread impact to facilities / sites and / or business / economic stakeholders
Catastrophic Level 5	Direct loss or increased cost of over USD100,000	Significant regulatory enforcement action and intervention (e.g. Revocation/suspension of license, criminal or civil action taken against company, Executive Committee or directors.	Cessation of core activities for more than one week. Significantly affects key business stakeholders.	A large number of senior managers / experienced employees leave. Loss of life involving corporate negligence.	Prolonged negative media exposure likely to prompt regulatory investigation. Total loss of public confidence and reputation.	Most customers suffer problems that causes them major inconvenience. Affects > 100 customers requiring redress or correction. Loss of cover critical client information across policies where the aggregate liability exceeds USD5,000 or failure in systems to record	Catastrophic damage or loss of FWD physical assets or property Catastrophic impact to facility or property security.

		Multiple related intentional breaches of internal governance document.			Major loss of shareholder, political or community support.	policies where the aggregate liability exceeds USD30,000	Impact on all facilities / sites and / or business / economic stakeholders
--	--	--	--	--	--	--	--

### 8.3 Risk Level

The Risk Level is determined by combining Impact and Likelihood dimensions of risk. The Risk Level can also be quantified in monetary terms but would be used for comparative purposes only and will be meaningful only if Likelihoods and Impacts have been assessed consistently.

Likelihood	Impact Rating				
	Level 1 Insignificant	Level 2 Minor	Level 3 Moderate	Level 4 Major	Level 5 Catastrophic
A. Almost Certain	Yellow	Orange	Red	Red	Red
B. Likely	Yellow	Orange	Orange	Red	Red
C. Possible	Green	Yellow	Orange	Red	Red
D. Unlikely	Green	Green	Yellow	Orange	Red
E. Rare	Green	Green	Green	Yellow	Red

**Extreme:** These risks exceed tolerance levels and are so significant in the context of the business objectives and/or value drivers impacted that management should determine any exposure to date and, without delay, inform the next level of the Company;

**High:** These risks exceed tolerance levels. Resources need to be assigned to mitigate risks within a reasonable time frame. Next level of the Company needs to be informed;

**Moderate:** These risks are important in the context of the business objectives and/or value drivers impacted, but do not exceed tolerance. Management should develop action plans that will ensure timely mitigation of the risks. Monitoring is required to avoid worsening situations;

**Low:** These risks are not currently material in the context of the business objectives and/or value drivers impacted, but management should monitor the risks and take appropriate action, as necessary, to prevent the risks from becoming material.

C2 - Internal



# FWD Life Insurance (Cambodia) PLC. Enterprise Risk Management Policy

<b>Document ID</b>	KH-CG_RM-PO-0001	<b>Document Type</b>	Policy
<b>Issued by / Owner</b>	Chief Legal and Compliance Officer	<b>Approved By</b>	Board of Directors
<b>Target Audience</b>	Directors, all risk owners, employees, agents and contractors		
<b>Document Status</b>	In-Effect	<b>Last Approved Date</b>	27 <sup>th</sup> April 2022

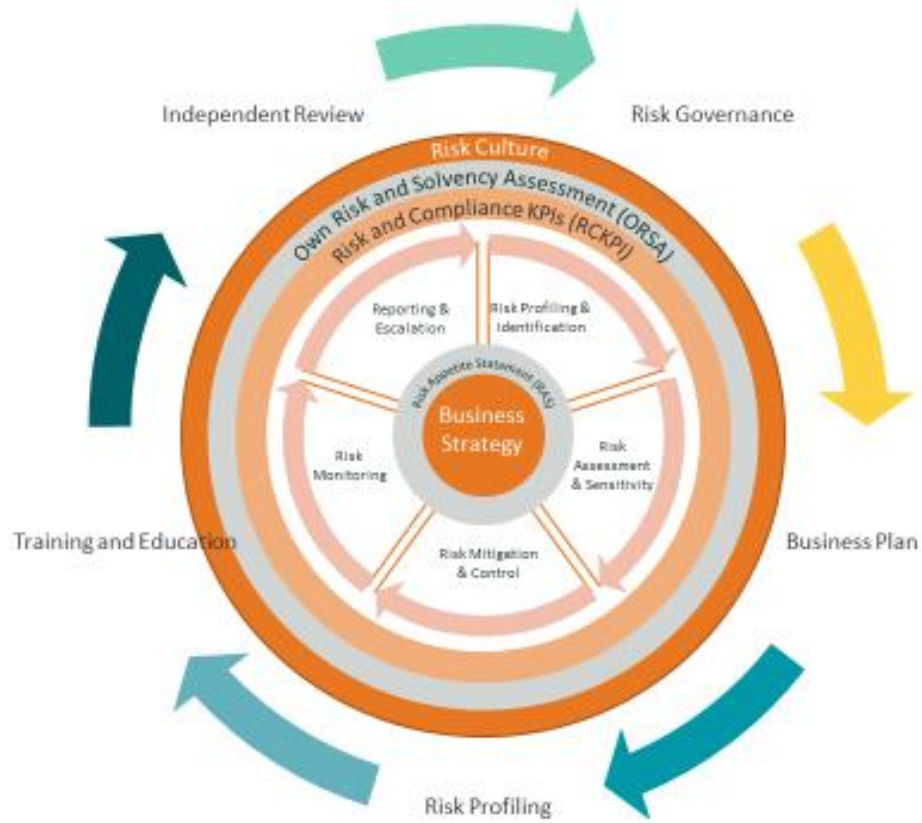
## Document Approval History

Version	Date Approved	Description
1.0	27 <sup>th</sup> April 2022	First version

## Table of Contents

1.	Introduction .....	4
2.	Review.....	4
3.	Scope .....	4
4.	Business Vision and Strategy.....	5
5.	Risk Governance and Organisation .....	5
6.	Risk Appetite.....	6
7.	Risk Culture.....	7
8.	Business Plan.....	7
9.	Risk Profiling .....	8
10.	Risk Identification.....	9
11.	Risk Assessment Approach .....	12
12.	Risk Mitigation & Control.....	15
13.	Monitoring .....	17
14.	Escalation.....	18
	Appendix 1: Definitions .....	21
	Appendix 2: Classification of Risks .....	24

# ERM Process Diagram



## 1. Introduction

FWD Life Insurance (Cambodia) PLC. (hereafter termed as “FWD” or “Company”) is a financial services company that provides protection and wealth management products and services to end consumers. This exposes the Company to a variety of risks that needs to be managed accordingly.

This document aims to provide principles and strategies for implementing the Enterprise Risk Management Framework (ERMF). This document should be read in conjunction with the Risk Appetite Framework (RAF) and the ERMF to proactively manage risks in a holistic fashion. This is a policy document and does not include details on the approach for managing each category of risk.

The diagram on page 3 provides a high-level flowchart of the Enterprise Risk Management (ERM) environment and processes to guide all staff in FWD on implementing different components of the risk management process across the business. This document provides requirements for executing each step of the ERM environment and processes.

## 2. Review

This Policy should be reviewed at least annually to ensure continued appropriateness to the Company. The review is to be conducted by the Head of Risk (or equivalent) and should be approved by the Board of Directors (hereinafter referred to as the “Board”).

## 3. Scope

This Policy applies to the Company as a whole. Any non-compliance of this Framework should seek the approval from the Board of Directors and Group Office.



## 4. Business Vision and Strategy

FWD is focused on creating fresh customer experiences, with easy-to-understand products, supported by leading digital technologies. Through this customer-led approach, FWD will achieve our vision, changing the way people feel about insurance.

## 5. Risk Governance and Organisation

The Chief Executive Officer (CEO) delegates day to day management of risk to Management in their respective business and functions. Management is supported by central specialist risk functions, Chief Compliance Officer and the Head of Risk (or equivalents). The Enterprise Risk Management Framework has articulated the Risk Governance structure in FWD. The Company is required to adopt a *3-lines of defence model* and proper risk governance structure must be established for FWD.

### 5.1 Framework / Delegated Authority / Policy / Standard Setting

Company frameworks, delegated authority, policies and standards are in place to assign the approval authority and to manage the significant risks that FWD runs as an organisation. They are one of the key building blocks of organisation control which form the base in managing key risks and at the same time be beneficial in running the business to deliver the Company's strategy. Risk owners are required to develop the frameworks, policies and standards to manage risks in the respective responsible areas in accordance with the Delegated Authority.

### 5.2 Chief Compliance Officer and Head of Risk

The Chief Compliance Officer and Head of Risk (or equivalents) should be independent from operations and have unrestricted access to all staff, systems and information needed to perform their role. The Chief Compliance Officer and Head of Risk are responsible for developing and executing the Enterprise Risk Management Framework.

### 5.3 Reporting lines of local 2<sup>nd</sup> line functions

The Company should appoint a Chief Compliance Officer and Head of Risk (or equivalent)

. Apart from the local reporting line into local Management and local Audit Committee, the Chief Compliance Officer and Head of Risk should have a dotted reporting line into Group CRO and Group CCO respectively. The appointment and termination have to be agreed by local Management and Group CRO and Group CCO respectively.

## 6. Risk Appetite

The objective to establish risk appetite for FWD is to ensure that appropriate governance, reporting, limits and decision processes have been set up, to facilitate the consideration of underlying risks when making management decisions. It is a structured process to ensure consistency of risk tolerance, to have a clearly stated risk appetite by articulating the aggregate level and types of risk the Company is willing to take within its risk capacity to achieve its financial & strategic objectives and business plan, to monitor the accumulation of risks, and to manage its exposure on a regular basis.

The methodology and the components for developing a Risk Appetite Statement (RAS) are presented in the ERMF and Risk Appetite Framework (RAF). To ensure the RAS is operationalized in business strategy and day-to-day operations, the Company must develop risk metrics to measure the risk limit against the risk tolerance and report to Audit Committees and Board at least quarterly or on a timely manner.

Governance around risk appetite is expressed by setting “Low”, “Medium”, “High” and “Extreme” limit levels (as demonstrated in the below diagram) on risk metrics, leading to regular tracking of exposures to ensure they are within limits or appropriate escalation and actions are taken as per below to resolve breaches, if any.

<b>Low (Accept the risk with routine risk reporting)</b>	<b>Medium (Accept the risk with routine risk reporting. May require some management actions)</b>	<b>High (Accept the risk and immediate notification to the Risk Committee Chair. Immediate mitigation actions needed)</b>	<b>Extreme (Immediate escalation to the Board along with mitigation actions required)</b>
--	--	---	---

Breaches of risk appetite limits (i.e. High or Extreme) must immediately be reported to Group CRO and Audit Committee (High) or Board (Extreme). Regular reporting on quarterly exposure versus appetite is embedded in the Quarterly Risk Management Report.

## 7. Risk Culture

Risk culture is the set of shared values and behaviours of all staff in FWD that influence risk decisions. The Company aims to maintain a risk culture which enables proactive management of risk by all staff across the organisation.

At FWD, we believe that the “tone from the top”, leadership engagement, accountabilities and awareness and communication initiatives are key to ensure that a strong risk culture is prevalent across the organisation. A visible focus on risk at the highest level of management emphasises the importance of and encourages risk awareness. This is demonstrated through FWD’s commitment toward the three lines of defence risk governance model.

## 8. Business Plan

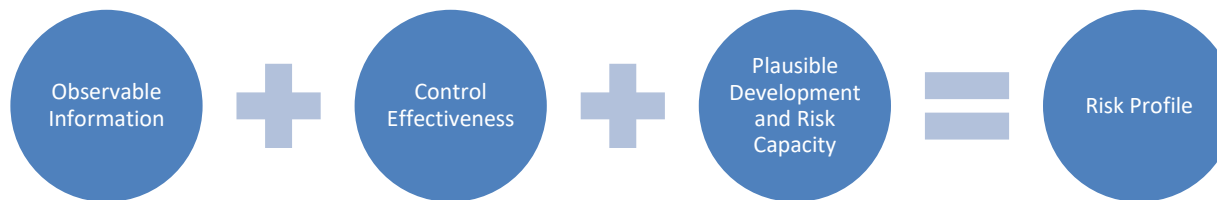
As part of the business planning process, Head of Risk should facilitate respective Executive committees to conduct both qualitative and quantitative risk assessment to identify risks that may significantly impact the delivery of the business plan and risk profile of the Company.

The qualitative risk assessment can use either “top-down” or “bottom-up” approach, and it should focus on the Company’s business strategy and consider external operating environment as well as regulatory landscape. Quantitative risk assessments should consider the availability and credibility of data as well as judgement of the Chief Actuary. Based on the result of these assessments, the Executive Committee should document the identified risks and mitigating actions (e.g. recovery plan) in the business plan, and the information should be submitted to the the Audit Committee or the Board for noting. Key Risk Indicators should also be set up, monitored and reported for the top risks identified.

If a risk is assessed to be outside risk appetite and no further mitigation actions can reasonably be taken to lower the managed risk level within appetite, such risks must be escalated by the respective risk owner to the Group CRO and local Audit Committee or Board in accordance with the requirements specified under “Risk Acceptance” section of this policy.

## 9. Risk Profiling

The overall risk profile is the aggregation of total risk considerations of the Company. The Company must assess the risk profile of each underlying risk category and report to Group Risk and the Audit Committee on at least quarterly basis or as otherwise agreed with Group Risk. The risk profiling exercise should be conducted more frequent if any change in risk drivers may materially impact the risk profile of the Company. The assessment of risk profile should consider the combination of all available information, the effectiveness of control environment, plausible change of the circumstances and the capacity of the Company to absorb the risks.



### 9.1 Observable Information

Each risk owner has to use a set of information as the starting point to assess the risk profile of the Company. The set of information can be observed:

- The trend of Risk Appetite Metrics
- The trend of key risk indicators including economic indicators and experience analysis.
- Incident and issues, taking into consideration of the trend and concentration of the issues which might become potential systemic problem in the organisation
- Change of external (e.g. regulatory changes, etc) and internal (e.g. change in business strategy, major M&A, etc) operating environment

## 9.2 Control Effectiveness

While assessing the risk profile, the risk management function should form an independent view of the effectiveness of the controls and mitigation actions to assess the risk profile. This independent view should take into consideration design and operating effectiveness assessed for example through analysis of incidents, monitoring, process walkthroughs or testing performed by the 1<sup>st</sup>, 2<sup>nd</sup> or 3<sup>rd</sup> line of defence. Where applicable there should also be an assessment of whether mitigating management actions could reasonably reduce residual risk ratings.

## 9.3 Plausible Development and Risk Capacity

The risk profile should take a forward looking view. The assessment should take into consideration emerging matters (internal and external factors) that may plausibly affect the trend of the observable information in either positive or negative direction. The Risk Owner should evaluate the Company's ability to accept further risks.

# 10. Risk Identification

## 10.1 Risk Identification

Risks are identified by using open-end assessment or closed-end assessment as per the ERMF and the relevant risk management policies. All identified risks should be recorded in the ERM Risk Register (see next section) to ensure proper tracking of the mitigation actions and for future analysis purposes.

Examples of Open-end and Closed-end Risk Assessment:

- a) Open-end assessment – broad in scope and wide varieties of risks, usually performed on a periodical basis
- b) Closed-end assessment – questionnaire-based and specific risks, usually performed upon an event trigger

## 10.2 ERM Risk Register

The Company must maintain an ERM Risk Register covering the key risk categories to which the business is exposed. Whilst the precise approach to the assessment of risks will vary by category and maybe set out in specialist risk management policies, the risk assessment principles set out in this policy must be adhered to.

The ERM risk register must include an assessment of inherent risk, managed risk, and residual risk against the four risk ratings: extreme, high, moderate, and low.

The assessment of risk should consider at least the following perspectives.

All risks should have an identified owner to ensure accountability. Whilst risk management and other key control functions may coordinate, or support the assessment of risks, risk owners are responsible for the final assessment result, effectiveness of controls and associated action plans.

The Company must assess the totality of the risks at least annually in line with the assessment of the Business Plan risks deriving an overarching risk profile and an agreed upon set of key risks. These key risks must be routinely reported on to the Group Risk team.

The ERM Risk Register is the Executive Committee's assessment of its risks. The ERM Risk Register is a repository for all risks identified to which the Company is exposed as a result of executing the business strategy. . As the business evolves, the risk register should be updated correspondingly based on the changes (e.g. new or updated strategy/initiatives, new issues/incidents identified, change of external environment, etc.). The ERMF has specified the outcome of the risk assessment which includes three stages (i.e. Inherent risk, Managed risk and Residual risk) and four Risk Levels (i.e. Extreme, High, Moderate and Low). This section provides guidance in conducting an Open-end (or "top-down") Enterprise Risk Assessment.

The Executive Committee, supported by Risk Management and Compliance, is responsible for planning and facilitating the assessment process. All risks identified must be recorded in the Group system (e.g. Archer or ServiceNow, as appropriate).

The report setting out the annual ERM risk assessment must be reported to Group CRO and include the key risks arising from this assessment, and any significant change in the risk profile and impact to the top risks of the Company which will be routinely reported on.

A scenario-based approach should be applied in describing a risk. A scenario must be specific and not generic and must describe the background and context of a risk situation. It should document why such scenario is deemed as critical and significant for FWD.

The approach to risk assessments may vary by risk type. However typically, the assessment would include a mixture of one to one interviews and/or workshops involving the first line of defence. Risk identification must consider all scenarios which prevent business objectives from being achieved.

At the minimum, the following questions must be asked during the risk identification process:

- What are the key business initiatives in the business? What could prevent these initiatives from being achieved as planned by considering both internal and external factors?
- What statutory obligations do we have and what could threaten these e.g. minimum capital requirements, or the fair treatment of customers.
- What are the key business processes and key controls in the department? What could prevent these processes and controls from being effectively executed?
- What are the expectations of customers? What could stop me from meeting these expectations?
- What does my history tell me (e.g. past incidents/losses/issues, results of Key Controls Self Assessment (KCSA), Key Risk Indicator trends)?
- What incidents have affected my competitors?
- Who do I rely on (e.g. key third party vendors) to deliver services to my customers?
- Are there any external developments (market, technology, regulatory, etc.) that could impact the business?
- What issues (if any) have Internal Audit, Risk or Compliance identified?
- Management's knowledge and observations of their business
- What issues have been identified in Closed-end Assessments?

Classification of risks as listed out in Appendix 2 and provides a control checklist to ensure all relevant types of risk have been considered in risk identification.

### 10.3 Emerging Risk

Emerging risks are newly developing or changing risks which may have a major impact on society and the insurance industry. These risks are difficult to quantify and their potential business impact cannot yet be fully estimated with any certainty.

The objective of emerging risk management is to establish a process to identify and monitor these risks, analyse their significance and prepare for and/or potentially mitigate them. The pro-active screening process helps FWD to anticipate future threats.

In order to ensure that the emerging risk management process provides full coverage of FWD's environment, an external screening process should be developed that draws on various sources including:

- Regulatory updates
- Emerging risk reports from global bodies
- Industry forum and private firm emerging risk reports
- Media reporting and external events

All relevant Emerging Risks should be discussed among local Executive Committee and Group Risk.

## 11. Risk Assessment Approach

As specified in the Enterprise Risk Management Framework, risks are assessed in two dimensions –likelihood and impact, and then classified into the one of the four risk levels (Extreme, High, Moderate or Low).

### 11.1 Risk Acceptance

A risk is considered to be accepted when management do not want to take further mitigation actions to lower the managed risk level. Acceptance of a risk outside appetite (i.e. managed and/or residual risk level rated as Extreme or High) or beyond



risk limits specified in other policies or standards should however be a rare event and any decision to accept risk must be escalated by the risk respective owner to the relevant risk committee(s) or Board in accordance with the requirements under Risk Appetite Framework.

A risk acceptance log should be maintained, and all risk acceptance activities at the Company must be reported to Group CRO (and Group CCO for compliance risk related risk acceptance) before they are being submitted to the relevant risk committee(s) or Board for approval.

The maximum validity duration of the approved risk acceptance is 12 months. This procedure must be executed again if the validity duration expires and the risk remains to be beyond appetite. It will also be necessary to gain robust assurance through regular review that existing controls, if any, are fit for purpose in order to be sure that the level of risk exposure is not any greater than first assessed.

For risks which are rated within the risk appetite and limits, risk acceptance is documented through recording the risk and the information as required on the Risk Register.

Accept:	<ul style="list-style-type: none"> <li>• The risk is within the Board defined appetite</li> <li>• There is a clear risk ownership of each risk</li> <li>• The risk can be managed by reducing the impact and/or likelihood either collectively or individually</li> <li>• We have sufficient knowledge and skillset to manage the risks</li> <li>• Using stress and scenario testing</li> <li>• regulatory capital, liquidity stress while the risk is quantifiable.</li> <li>• We have the risk capacity to absorb the risks</li> <li>• There is a plan to manage the severe situations</li> </ul>
Avoid:	<ul style="list-style-type: none"> <li>• The risks exceed Board defined risk appetite</li> <li>• No risk owner can be identified</li> <li>• The risks would potentially and materially change the risk profile of the Company and risk assessment has not properly conducted</li> <li>• Risk capacities are not available to accept such risks</li> <li>• The risks are not understandable and manageable</li> <li>• Material risks have not passed through the risk governance process</li> </ul>

## 11.2 Likelihood

Assessing the Likelihood dimension of risk involves considering how frequently the incident or event may occur over a specified time horizon. The typical Likelihood scale is characterized by 5 qualitative descriptive scales.

## 11.3 Impact

It is important to recognize that the consequences of any particular risk event may impact in different ways: financial costs; personal harm; legal consequences; and damage to reputation may all result from a single incident.

## 11.4 Risk Level

The Risk Level is determined by combining Impact and Likelihood dimensions of risk. The Risk Level can also be quantified in monetary terms but would be used for comparative purposes only and will be meaningful only if Likelihoods and Impacts have been assessed consistently.

Qualitative and Quantitative risk analysis matrix- level of risk

Likelihood	Impact Rating				
	Level 1 Insignificant	Level 2 Minor	Level 3 Moderate	Level 4 Major	Level 5 Catastrophic
A. Almost Certain	Yellow	Orange	Red	Red	Red
B. Likely	Yellow	Orange	Orange	Red	Red
C. Possible	Green	Yellow	Orange	Red	Red
D. Unlikely	Green	Green	Yellow	Orange	Red
E. Rare	Green	Green	Green	Yellow	Red



## 12. Risk Mitigation & Control

If the risks are considered acceptable by the Company, the Management must agree the risk mitigation actions, taking into consideration of the risk appetite, the policies and standards, scale of business and cost to implement appropriate controls in the respective business units. All risks and their mitigation actions must be recorded in the Risk Register for systematically tracking implementation progress of the actions identified through the Risk Profiling, Controls and monitoring phases of the ERM process. Mitigating actions should be assigned with both anticipated completion date and action owner(s).

### 12.1 Guidelines to formulate risk mitigation and control

The risk/process/incident/issue owner is ultimately accountable for coordinating and agreeing mitigating actions with relevant functional areas, and risk/process/incident/issue owner does not have to be the action owner and can be a different person. Collaboration with other functional areas should be agreed as required.

Risk Mitigation Strategies	
<ul style="list-style-type: none"> <li>Reduce</li> </ul>	<ul style="list-style-type: none"> <li>The risk owner and action owner should work with Management to manage the risk down to the residual risk level that is acceptable to the Company. It involves countermeasure to decrease the likelihood or impact of consequences.</li> </ul>
<ul style="list-style-type: none"> <li>Transfer</li> </ul>	<ul style="list-style-type: none"> <li>In certain circumstances, risks can be transferred because of limited knowledge, economic of scale, or limited risk capacities. The following are typical examples for risk transfer:               <ul style="list-style-type: none"> <li>Leveraging the reinsurer by ceding certain insurance risks to reinsurer, that FWD has limited capacity and/or knowledge of the insurance risks;</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Using derivatives as a tool to manage the risk exposures and minimize capital consumptions, which FWD will not take significant market positions;</li> <li>• Outsourcing certain procedures to leverage the vendor's knowledge and to achieve economic scale, while FWD remains the full accountable of outsourced procedures;</li> <li>• Fronting arrangement with business partners.</li> <li>• Transferring risk to a 3rd party may reduce the risk exposures in respective area. Such arrangement however may induce a new risk in other area, such as counter-party default risks, reputation risks, etc. All these new risks should follow the risk management process that assign a clear risk owner, identify the mitigation action, evaluate the risk level and record in risk register accordingly. In particular, the Company should take into consideration of the following factors where appropriate: <ul style="list-style-type: none"> <li>• the economic impact of the risk transfer originating from reinsurance contracts by the Company with sufficient documentation to address the substance of the risk transfer;</li> <li>• addressing any issues that may arise as a result of risk transfer to capital markets including an understanding and assessment of the structure and operation of such risk transfer arrangements;</li> <li>• establishing a robust framework in managing and monitoring the alternative risk transfer ("ART") arrangements to ensure it is adequate and appropriate to the nature of the underlying risks and to the complexity of the ART arrangements; and</li> <li>• assessing the effectiveness of risk transfer arrangements in adverse circumstances.</li> </ul> </li> </ul>
--	---

Action plans must be SMART (Specific, Measurable, Achievable, Relevant and Time bound) and should include actions that have previously been identified to address existing issues (e.g. regulatory or legislative breaches or internal audit findings).

Overdue actions are significant for FWD as they represent a continuing risk exposure beyond that anticipated with the potential for further opportunities missed or downside impact such as financial loss, reputational damage and/or regulatory censure. They may also impact other areas dependent on the fix which creates unforeseen exposures for the area.

The action owner is responsible for ensuring their action plan remains on track. Actions that have or are expected to not meet their due date must be escalated by the action owner to risk/process/incident/issue owner and Risk Management. A clear explanation of the root cause and evaluation of the risk profile as a result from the overdue item should be supplemented. Risk Management should provide the CEO, relevant risk committee(s) and Group Risk Management with the mitigation actions tracking report on a quarterly basis. Where a delay is deemed unacceptable, risk/process/incident/issue owner should agree a revised and acceptable time frame for the action plan with Risk Management.

An action can only be closed once the risk/process/incident/issue owner is satisfied the action is completed to a satisfactory standard. The risk/process/incident/issue owner should obtain assurance from the action owner that any improvements or remediation are in place or completed and are effective. The risk/process/incident/issue owner should seek evidence from the action owner to confirm this. Risk Management's confirmation is required for action closure except for internal audit findings/issues which the respective action closure is to be confirmed by Internal Audit.

## 13. Monitoring

All risk owners are required to set up risk limits for selected key areas to manage business within the agreed risk tolerance. Risk Management function should monitor risk limits at least quarterly or in a timely manner. The report of risk limits should be submitted to Management. Any violation of risk limits should immediately be escalated to the Executive Committees for the mitigation actions and be reported to Group Risk Management. The proposed mitigation actions should be submitted to the Board or relevant Committee for approval.

Risk Management, with the support from the Executive Committee, has to propose the risk limits to relevant Committees and Group CRO for endorsement.

### 13.1 Key Risk Indicators (KRI) Setting

KRIs are metrics used to monitor identified risk exposures and, or to evaluate risk level of the Company over time KRI should not only be used in isolation and must be used as part of the risk assessment process, to provide more depth to the residual risk assessment and to inform the response to that top risk (e.g. accept, reduce, etc.). There can be several indicators feeding into one risk to inform the assessment.

KRIs should be established for all top risks where the gross or residual risk is high identified through the risk assessment process. Consideration should be given to metrics that demonstrate a potential increase or decrease in likelihood or impact of the specified risk.

Once suitable KRIs have been identified and agreed between respective first line risk owner and Head of Risk (or equivalent), limits should be set for each KRI. Limits (e.g. operational loss or service impact limits) are a mechanism for risk owners to articulate their risk tolerance(s) for individual risks (within the overall agreed risk appetite framework). The thresholds should be expressed by setting “Low”, “Medium”, “High” and “Extreme” limit levels.

When a KRI has been reported as “High” or “Extreme”, the indicator is providing a forewarning to management that their upper tolerance for a defined threshold has been crossed and as such should be investigated to allow the taking of proactive action to reduce the impact and/or likelihood of the risk materialising.

There should be at least an annual review of the KRI and their respective limits. They should be presented to the relevant risk committee(s) as part of the overall risk reporting.

## 14. Escalation

On quarterly basis, the Head of Risk (or equivalent) should evaluate the risk rating and profile of the Company. The risk rating and profile form part of the Quarterly Risk Management Report which will be submitted to Audit Committee and Group CRO. The Head of Risk (or equivalent) must submit the Quarterly Risk Management Report to the Group CRO as per the dates specified by Group Risk.

## 14.1 Escalation Process

The following table provides additional minimum requirements for mitigating actions depending on managed risk rating:

Managed risk rating	Action requirements
Extreme Risk	Immediate escalation to Group, Risk Management and Compliance by risk owner along with mitigation actions is required. Group, Board and CEO should be immediately notified on the risk.
High Risk	Immediate escalation to, Risk Management and Compliance by risk owner along with mitigation actions is required. Group and the Company's CEO and Chair of Audit Committee should be immediate notified on the risk. Respective Board and Risk Committee(s) are informed through regular risk reporting process.
Moderate Risk	The risk owner to inform the respective Executive Committees, Risk Management within one month of identification. For compliance risk, immediate escalation to Compliance and Group Compliance is required. Audit Committee is informed through routine reporting.
Low Risk	The risk owner to determine if the existing controls are sufficient to manage the risk or if additional mitigation or control improvement is required to prevent the risk from becoming material.

## 14.2 Mitigating Action Tracking



## Appendix 1: Definitions

TERM	DEFINITION
Impact	A factor for measuring risk that considers the different consequences which may result if a risk were to occur. This is considered alongside Likelihood for assessing inherent risk and residual risk.
Inherent Risk	Assessment of risks assuming that no controls exist. Assessment of inherent risk is recommended as it gives a good understanding of the gross exposure to the activity, and shall be based on incident data (scenario) analyses.
Key Control Self-Assessment (KCSA)	An assessment process performed by the Functional Unit to self-assess the quality of controls in place to manage risks arising in the Functional Unit.
Key Performance Indicators (KPI)	A quantitative measure used to gauge the performance of an individual. KPIs should be designed to be risk-based to encourage sound risk management practices and discourage excessive risk taking.
Key Risk Indicators (KRI) /Risk Indicator	<p>A quantitative measure used to gauge and monitor the riskiness of a risk. KRIs can be designed to gauge risks on a backward looking manner (i.e. monitoring past performance to gauge trends in certain risk areas) or on a forward looking manner (i.e. monitoring business trends which may have a flow-on impact to risk areas).</p> <p><i>Note: Key Risk Indicators and Risk Indicators are used interchangeably throughout the business.</i></p>
Likelihood	A factor for measuring risk that considers the expected frequency for a risk over a specified time horizon. This is considered alongside Impact for assessing inherent risk and residual risk.
Managed Risk	Assessment of the risks in their current control environment. Assessment of managed risk requires the identification of all relevant existing controls and the assessment of the control's effectiveness. Analysis/evaluation of the difference between the inherent and managed risk can provide a good understanding of effectiveness of the existing controls
Residual Risk	Assessment of the risks in their current control environment and future mitigation actions. For each possible future mitigation action a cost/benefit analysis shall be performed. Extreme and High residual risks should be escalated to the Group to determine how they are to be

	managed. Moderate risks are tolerated and can be accepted. Low risk is acceptable risk.
Risk	The possibility of positive or negative deviations to expectations when trying to achieve an objective.
Risk Acceptance Procedure	The detailed procedures for accepting risks. This includes the governance process when considering whether to take on a risk which is within or exceeds the Board's risk appetite.
Risk Limits	<p>Risk limits refer to metrics set by Functional Units to facilitate the measure of risk at an operational level. The metrics are done at a granular level relative to Risk Tolerance (which is set by the Board).</p> <p><i>Note: Risk limits and Risk Metrics are used interchangeably throughout the business.</i></p>
Risk Owner	Person or persons who are responsible for monitoring and managing a particular risk. This is maintained in the Risk Register.
Risk Preferences	A series of The Board's appetite for risks expressed as a set of qualitative statements linked to the key risk categories that the business is exposed to.
Risk Profile	An evaluation of an organisation's willingness to take risks that the organisation is exposed to.
Risk Tolerance	<p>The Risk Tolerances refer to the level of risk that the Board is willing to accept to achieve business objectives. The risk level definitions are, when possible, measurable and are used to monitor the business' performance against the Board's risk appetite.</p> <p>The Risk Tolerances apply quantitative measures to the Key Business Objectives (defined elsewhere). The quantitative measures are based on forward looking assumptions.</p> <p>The quantitative statements are expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate.</p> <p><i>Note: Risk Tolerance may have been referred to as 'Risk Level Definition' in earlier risk documents</i></p>
Three Lines of Defence (3LoD)	A governance structure that aims to facilitate sufficient risk oversight, challenge and assurance across all business matters.

	<p>The first line comprises all management and employees who manage risk day-to-day in accordance with the strategies and policies set by the Board. The second line comprises risk management and compliance to serve as an independent oversight of risk exposures and risk management practices. The third line comprises the audit functions (internal and external) to provide independent assurance on the design and effectiveness of the overall system.</p>
--	--

### Document glossary

Enterprise Risk Management Policy (ERMP)	The ERMP provides operational information for employing the Enterprise Risk Management Framework and other risk documents across the business.
Risk Appetite Framework (RAF)	<p>The RAF refers to the overall approach, including policies, processes, controls, and systems through which risk appetite is established, communicated, and monitored. It includes a risk appetite statement, risk tolerance and risk limits, and an outline of the relevant roles and responsibilities of those overseeing the implementation and monitoring of performance against the RAF.</p> <p>The RAF aligns with the Company’s strategy and should consider material risks to the Company.</p>
Risk Appetite Statement (RAS)	The Risk Appetite Statement is a key document for guiding all key business decisions, including strategy and capital. It includes qualitative statements (risk philosophy, risk preference, key business objectives) and quantitative statements (risk tolerances).
Enterprise Risk Management Framework (ERMF)	The ERMF refers to the overall framework necessary to identify and manage risks. It also covers establishing the risk appetite, which is an expression of the level of risk FWD is prepared to take to achieve its strategic objectives. It also establishes the risks FWD wish to acquire, avoid, retain and/or remove in pursuit of these strategic objectives.
Risk Register	A register containing results of risk assessments performed on all key risks in the business.

## Appendix 2: Classification of Risks

As shown in the table below, all risks the business is exposed to are classified into four major risk categories. These are in turn broken down into a number of lower level risk factors or risk issues.

Enterprise Risk Management			
Strategic Risks	Insurance Risks	Operational Risks	Investment, ALM & Capital Risks
<ul style="list-style-type: none"> <li>Group</li> <li>Channel</li> <li>Reputation</li> <li>Business Intelligence</li> <li>Technological Strategy Risk</li> <li>Political and Social</li> <li>Environmental and Climate</li> </ul>	<ul style="list-style-type: none"> <li>Mortality</li> <li>Morbidity</li> <li>Persistency</li> <li>Expense</li> <li>Underwriting</li> <li>Claim</li> <li>Pricing</li> <li>Model*</li> </ul> <p>*Focus purely on the non-operational risk aspect of model risk (e.g. appropriateness of assumptions setting, risk selection criteria that aligning assumptions)</p>	<ul style="list-style-type: none"> <li>People</li> <li>Fraud</li> <li>Physical Security and Safety</li> <li>Business Continuity</li> <li>Transaction Processing &amp; Execution</li> <li>Technology</li> <li>Conduct</li> <li>Legal</li> <li>Financial Crime</li> <li>Regulatory Compliance</li> <li>Privacy</li> <li>Third Party</li> <li>Information Security (including Cyber)</li> <li>Statutory Filing and Tax</li> <li>Data Management</li> <li>Model*</li> </ul> <p>* Focuses purely on the operational risk aspect of model risk</p>	<ul style="list-style-type: none"> <li>Liquidity / Surrender</li> <li>Interest</li> <li>Market</li> <li>Credit</li> <li>Asset Concentration</li> </ul>

### Strategic Risks

Strategic risks cover corporate level issues the FWD faces, particularly those related to the competitiveness and sustainability of the Company. Strategic risks also address issues that involve the long term direction of the FWD .

### Group Risk

Group risk refers to risks arising from being a member of a group. This considers the risks of an event/s to a group as a whole or to individual members which can adversely impact other members of the group. Group risk considers the inter-relationships between members of the group including control, influence and interdependencies.

## Channel Risk

Channel or sales channel is the primary contact point between FWD and its customers or policyholders. Channel risk is highly associated with the ability to attract and retain customers through the product offerings. To some extent, channel risk also deals with the quality and competitiveness of its contact with customers which often lead to many related risks, particularly those related to operational risks.

## Reputation Risk

Reputation risk refers to risks arising from any potential negative perception from customers, regulators, or counterparties regarding its business practices, regulatory compliance, and current and prospective financial status and/or solvency, including any indirect negative perception from its shareholders, investors or major business partners that could impair its ability to maintain/establish its existing/new relationship or service. Reputation risk could be caused by systemic or industry-wide factor in which FWD operates. Reputation risk usually results from other risk issues and cannot be quantitatively assessed in isolation.

## Business Intelligence Risk

Business intelligence risk refers to risks arising from a failure to adequately define, gather, analyse, and distribute intelligence about products, customers, competitors, and any aspect of the environment needed to support FWD executives and managers making strategic decisions. It is the organisational function responsible for the early identification of risks and opportunities in the market before they become *obvious*.

## Technological Strategy Risk

Technological strategy risk refers to risks arising from a failure to leverage technology to provide solutions that meet new requirements, inarticulate needs, or existing market needs. This is accomplished through innovative products, processes, services and technologies.

## Political and Social Risk

The risk FWD faces because of political and social changes or instability in a jurisdiction, country or region.

## Environmental and Climate risk

Environmental risk refers to the risk posed by the exposure of the Company to activities that may potentially cause or be affected by environmental degradation.

Climate risk refers to the risk posed by the exposure of the Company to physical, transition or liability risks caused by or related to climate change.

## Insurance Risks

Many insurance related risk parameters are characterised by the following three risk components.

- **Volatility:** The risk that actual value differs from expected, assuming the best-estimate parameter is true. Volatility is the result of the randomness of the risk process.
- **Calamity:** The risk of a one-time claim of extreme proportions due to a certain major event, which is not caused by a change of the parameters. The event can be viewed as a one-year shock. Examples of calamity risk are epidemics, earthquakes, big flood, terrorist attack, etc.
- **Uncertainty:** The risk of parameter estimation as a result of statistical estimation errors and changes of parameter over time.

### Mortality Risk

Mortality Risk is associated with life expectancy. There are two types of mortality risk

- **Positive mortality risk:** the case where more insured die than expected, leading to higher claims than expected (typical in traditional whole life, endowment and term products), and
- **Negative mortality risk or longevity risk:** the case where insured's live longer than expected, leading to higher claims than expected (typical in pure endowment, annuity and pension products).

Mortality within one year (volatility and calamity) can impact the profitability of FWD in the year and future cash flows. The uncertainty component of mortality could lead to potential shortage of liabilities.

### Morbidity Risk

Morbidity Risk is associated with health events where FWD is exposed to indemnifying or reimbursing losses caused by illness, accident or disability, or for expenses of medical treatment necessitated by illness, accident or disability. Morbidity Risk comprises of the risk of variability of size, frequency and time to payment of future claims, development of outstanding claims and allocated loss adjustment expenses (ALAE) for morbidity product lines over the remaining contract period.

### Persistency Risk

Persistency Risk is the risk associated with adverse variations in persistency rates of policyholders from those in the best estimate assumptions. In all life insurance business the policyholder has the (one-sided) option to end the contract before the maturity date.

### Expense Risk

Expense risk is the risk that actual operational expenses in the future exceed the expected costs assumed in the pricing assumptions.

## Underwriting Risk

Underwriting risk arises from evaluating, assessing and accepting business or risks (insurance policy application) by underwriters which could result in poor or different portfolio behaviors than those assumed by pricing and reserving process.

## Claim Risk

Claim risk is the risk that the claim payment exceeds the claim reserve due to poor claim assessment and claim management, payment is made to invalid claims, including fraudulent claims.

## Pricing Risk

The Company's products usually have a very long maturity. Therefore, inadequate pricing of a product due to inaccurate assumptions, model or other calculation error can expose the Company to long term problems, e.g. loss, capital, which can't be easily resolved.

## Model Risk

The risk of adverse consequences (e.g. financial loss, poor decision making or damage to reputation) arising from the improper design, development, implementation and/or use of a model. The risk can originate from, among other things, incorrect parameter estimates; flawed hypotheses and/or assumptions; inaccurate, inappropriate or incomplete data; and inadequate monitoring and/or controls.

## Investment, ALM & Capital Risks

Investment & ALM risks are among the principal risks of an insurance company and key drivers of capital requirements.

### Market Risk

Market risk is the risk related to changes in the value of the assets, or asset cash flows, relative to changes in value of liabilities, or liability cash flows. It occurs when there is a mismatch between assets and liabilities due to different durations, sensitivity to changes in interest rates, foreign exchange etc.

Market risk may exist in life insurance companies as a result of selling products with guarantees or options (guaranteed crediting rates, surrender options, profit sharing, etc.) that cannot be hedged given the assets available in the market. Market risk may also occur when there is an intentional mismatch between asset and liability cash flows even when it is possible to match or hedge the cash flows.

### Credit Risk

Credit risk is the risk related to failure by the issuer, guarantor, reinsurer, or counterparty associated with a financial instrument or transaction to meet its obligations to pay principle or interest, settle claims, or make any other obligated pay-off.

### Liquidity and Surrender Risk

Liquidity risk occurs when FWD is unable to realise investments and other assets in order to settle its financial obligations when they fall due. Liquidity risk is an asset and liability concern; it is neither solely an asset nor a liability risk.

Surrender risk occurs when FWD experiences a suddenly unexpected cash outflows from policyholders' voluntary termination of their policy before its maturity.

### Asset Concentration Risk

A concentrated position refers to the significant presence of a single security, securities of a single issuer or a certain asset class or market segment relative to FWD's overall portfolio. Concentrated positions prevent diversification. A concentrated portfolio exposes FWD to the risks of portfolio underperformance, portfolio volatility, reduction in income and capital loss if forced to exit at wrong time.



## Operational Risks

The risk of loss resulting from inadequate or failure in internal processes, people and systems or from external events is defined as operational risk.

### People

Employment practice risk is the risk of loss due to acts inconsistent with employment, health laws, safety, or agreements.

### External Fraud Risk

External fraud risk is the risk of loss from dishonesty of individuals outside the Company, intended to defraud, misappropriate property or circumvent the law.

### Internal Fraud Risk

The risk of loss from dishonesty of personnel within the Company to defraud, misappropriate property or circumvent regulations, the law or Company policy.

### Physical Security and Safety

Losses arising from damage to physical assets from accidents.

### Business Continuity

Losses arising from inability to recover due to business disruption or system failure.

### Transaction Processing & Execution

Losses from failed transaction processing or process management due to relations with trade counterparties and vendors.

### Technology

Losses arising from technology failures, inadequate or failure in the management of technology systems and associated processes.

### Conduct

Losses arising or adverse consequences due to conducting insurance business in a way that does not ensure the fair treatment of customers, fair outcomes, or results in harm to customers.

### Legal

Losses arising from legal proceedings due to contractual or intellectual property disputes. Non-compliance with legislative requirement that lead to regulatory penalties or customer litigations.

## Financial Crime

Financial Crime Compliance (“FCC”) - Loss from any offence involving handling money or property that is from the proceeds of crimes or financing terrorism; the abuse of entrusted power for gain by offering (or promising to offer) or receipt of anything of value; failing to report the tax residence status; from any misconduct in or misuse of information related to a financial market.

## Regulatory Compliance

Losses arising or adverse impact to business operations from breach of regulation or industry practices and codes, ineffective and non-transparent relationship with regulators or failure to effectively implement regulatory changes.

## Privacy

Loss arising from inappropriate management of personal data.

## Third Party

Losses from failed transaction processing or process management due to relations with outsourcing vendors or suppliers.

## Information Security (including Cyber)

Losses arising from failure to safeguard Company and customer information.

## Statutory Filing & Tax

Losses arising from penalties or other financial penalties due to failure to meet regulator obligations in report tax filings.

## Data Management

Losses arising from poor data management, inadequate data analysis, unavailability of data, poor data quality, inadequate data architecture/IT infrastructure, inadequate data storage/retention and destruction management.

## Model

Losses arising from errors in design, methodology, implementation or application. Failure to detect changes, error inputs and outputs. Model risk is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model risk can lead to financial loss, poor business and strategic decision making, or damage to a reputation. Operational risk component includes misuse or errors in implementation, model governance breach, etc.