Module I Unit 15

COMPLIANCE

Purpose

At the end of this unit the participant should understand the importance of the compliance function and the role of the Compliance Officer.

Assumed knowledge

None

Summary of learning outcomes
1. Describe the compliance requirements of a licensed insurer
2. Describe the role of the Compliance Officer
3. Explain the concept of three lines of defence
4. Describe the key components of a compliance report to the board
5. Explain the role of the insurance manager with regard to AML/CFT
6. State the seven data protection principles to be observed
7. State the five core principles of the Cyber Rules

Module I Unit 15

COMPLIANCE

15.0 ROLE OF THE COMPLIANCE OFFICER

Licensed insurers are required to have an effective compliance function capable of assisting the board meet its legal and regulatory obligations and promote and sustain a corporate culture of compliance and integrity.

The Compliance Officer is required to:

1. Develop and maintain the appropriate compliance culture in the organisation
2. Develop and maintain processes and systems that help to ensure regulatory compliance and identify and deal with breaches
3. Advise the board and the Insurance Manager's client service team as to how to deal with regulatory issues
4. Update the board and the Insurance Manager's client service team on new or changed regulations and introduce new or revised processes to ensure compliance with the new requirements
5. Monitor the company's compliance with laws and regulations
6. Deal with regulatory and other breaches
7. Report to the board at each meeting on the level of compliance during the period since the previous report.
8. Liaise with the Commission on compliance questions, issues and breaches.

15.1 COMPLIANCE FRAMEWORK - 3 LINES OF DEFENCE

For managed companies the board will most often appoint the Insurance Manager as Compliance Officer. The function will usually be fulfilled by a member of the Insurance Manager's compliance team - one or more individuals who have no other operational responsibilities for the company so that they are able to act independently and provide appropriate oversight and reporting to the board. Some Insurance Managers outsource their compliance function to a third-party service provider.

As a managed company the board will typically adopt the Insurance Manager's compliance and risk management framework, policies and procedures as the company's own. The compliance and risk management framework would be expected to include three lines of defence:

1. The first line of defence - operational management - is provided by the Insurance Manager's staff who are involved in the day-to-day operations of the company. The staff should have the necessary skills, knowledge and authority to operate the relevant compliance and risk management policies and procedures. This requires training staff to ensure that they can perform their roles in a compliant manner, following policies, procedures and controls that will be effective in ensuring regulatory compliance and robust risk management.

2. The second line of defence - compliance specialists - will be the compliance team who develop and implement the policies and procedures, provide the necessary training, tools and support to the service teams in the first line and monitor the effectiveness of the controls through a compliance monitoring programme.

3. The third line of defence - independent assurance - is provided by internal audit. Its main roles are to ensure that the first two lines of defence are operating effectively and report to the board as to how they could be improved.

A Compliance Report should be tabled by the Insurance Manager at each board meeting which will assess and report to the board on the company's compliance with updates on all aspects of the relevant laws and regulations. Any breaches of regulatory concern will however be reported to the Board as soon as practicable after they are identified.

15.2 ANTI MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM (AML/CFT)

Guernsey's AML/CFT legal and regulatory framework is outlined in the GFSC's Handbook on Countering Financial Crime and Terrorist Financing.

The Handbook contains the relevant rules and guidance on how to implement them in practice using a risk-based approach.

Long term / life insurance business is subject to the Handbook rules**, but general insurance business is not. As such much of what follows does not apply to an insurer writing general insurance.**

- Life business has a higher risk of money laundering and financing terrorism than general insurance, as it may involve:
- high value single premium policies,
- investment, savings and top-up features,
- the ability to receive an annuity,
- to borrow against the value of the policy, or to surrender the policy and receive most of the cash back,
- and the ability to transfer or sell the policy to a third party or use it for collateral against a bank loan.

General insurance business is seen as low risk as the primary way that funds can be paid out is in the event of an insurance claim which will first be verified by the insurer as non-fraudulent.

The Handbook Rules relate primarily to:

- The policies procedures and controls that should be in place to support a risk-based approach to identifying, assessing, mitigating, managing and monitoring AML/CFT risk.
- The formatting, conducting and documenting of Business Risk Assessments which determine the firm's risk appetite, assess the risk associated with its customers, beneficial owners of customers, countries and geographic areas, products, services, transactions and intermediaries and determine how the risks are, or will be, mitigated.
- Customer due diligence that should be carried out to establish the identity of the customer and their beneficial owners, their activities and the source of their funds and wealth.
- The requirement for enhanced due diligence for any relationship assessed to be high risk including politically exposed persons (PEPs) such as heads of state, government officials, politicians and judges, and those in high-risk territories.
- Monitoring activity and ongoing customer due diligence.
- Screening for UN, UK and other sanctions
- Reporting suspicious activity to the Financial Intelligence Service (FIS)
- Employee screening and training

The board of a life insurer has responsibility for compliance with the Handbook and oversight of compliance, and where an outsourced service provider is being employed, including an Insurance Manager, then the board must ensure that the service provider has appropriate policies, procedures and controls in place to manage the AML/CFT risk effectively. Life insurers must submit an annual Financial Crime Risk Return to the GFSC.

Module I Unit 15

COMPLIANCE

The board must appoint the following:

1. **Money Laundering Compliance Officer (MLCO)** - a natural person (as opposed to a corporate appointment) at a senior level with the appropriate knowledge, skill and expertise who reports directly to the board.

The MLCO's role is to monitor the company's compliance with its policies, procedures and controls and report thereon to the board. The functions of the MLCO include overseeing the monitoring and testing of AML and CFT policies and procedures and investigating matters of concern or non-compliance and remediating issues where necessary.

2. **Money Laundering Reporting Officer (MLRO)** - a natural person at a senior level with the appropriate knowledge, skill and expertise who reports directly to the board and is the main point of contact with the Financial Intelligence Service (FIS) in the handling of disclosures.

The MLRO must have the authority to act independently and have direct access to the FIS to report any suspicious activity as soon as possible.

3. **Nominated Officer** who acts as MLRO in the MLRO's absence

Insurance Managers are also subject to the Handbook rules for their own business and will therefore need to appoint an MLCO, MLRO and nominated Officer and have procedures and policies in place for managing AML/CFT risk.

Therefore, although general insurance business carried out by companies under management is not covered under the Handbook rules, the Insurance Manager will need to ensure that the capital and premiums paid by the client to the insurance company are not the proceeds of crime, and that the transactions being carried out by the company are not financing terrorism. In addition, the board of a general insurer will still have a duty to ensure that the company is not being used for criminal purposes and to report any suspicions and will use the Insurance Manager's MLRO to investigate and report any such suspicions.

Insurance Managers will need to conduct a Business Risk Assessment on their client base, products, intermediaries, and territories at least annually. Due diligence will be undertaken on prospective new clients or where there is a change of shareholder for an existing client, to ensure that the identity and source of funds of both natural persons and corporate entities in the ownership structure, all the way up to the ultimate beneficial owners, are verified and risk assessed.

Insurance Managers will also ensure that their staff are screened as part of the recruitment process and provided with regular training - at least annually - to ensure that they understand how the Handbook rules apply to the business and to them as individuals. The training will include how to conduct adequate due diligence on prospective and current clients, identify suspicious transaction activity, when and how to report concerns to the MLRO, and how to avoid 'tipping off' the client that there are suspicions regarding their activity.

Individual staff may be committing a criminal offence if they do not report suspicious activity to the MLRO or if they tip off the client that an investigation is underway, and therefore it is important that they report any concerns to the MLRO immediately. The MLRO is then personally responsible for making the necessary disclosure to the FIS and for advising the staff members as to what if any further action to take.

The Insurance Manager may be an approved introducer for other financial services business such as banks and investment managers, whereby the bank or investment manager will be able to rely

upon the identification data and other documents obtained by the Insurance Manager from the client and beneficial owner, instead of having to obtain them directly from the client.

15.4: DATA PROTECTION

Data protection relates to the processing of personal data, i.e., data relating to an identified or identifiable living natural person (data subject), and the movement of such data between jurisdictions.

Data protection requirements in Guernsey are primarily governed by The Data Protection (Bailiwick of Guernsey) Law, 2017 (DP Law).

The DP Law was drafted to mirror the EU's General Data Protection Regulation (GDPR) in order to conform to EU standards and ensure that Guernsey continues to have 'adequacy' status as a third country, i.e. an adequate level of protection equivalent to that within the EU.

Adequacy enables the free flow of data flow between Guernsey and the EU, which is important for Guernsey's international insurance business given that many business relationships are with EU entities.

The Office of the Data Protection Authority (ODPA) administers the DP law in Guernsey and all insurers are required to register with the ODPA annually.

The DP Law requires the following seven data protection principles to be observed:

1. Lawfulness, Fairness & Transparency.
There must be a valid legal reason for processing personal data. It must be obtained without deceiving the person whose data it is, and it must be made clear exactly how the data will be used

The valid legal reasons are set out in the DP Law, and those which are most likely to apply to insurers are:

- Consent of the data subject, for example to receive marketing material.
- Contractual - the performance of a contract to which the data subject is a party or that is in the interests of the data subject. This applies to insurance policies and associated activities, such as claim handling.
- Law - the processing is necessary for the exercise of a right, power or duty imposed by law. This would apply to information collected to comply with the insurance licencing or AML/CFT requirements

A privacy notice must be issued to the data subject to provide certain information which will include the basis on which the data is required, what will happen to it and the rights of the data subject. The privacy notice may be included on the insurer's website and e mail footers and in proposal forms, policy documents and claim forms.

2. Purpose Limitation.
The personal data must only be used for the reason (or reasons) told to the person for whom it is being used.

3. Minimisation.
Only the minimum amount of personal data should be requested.

The insurer should consider if it really needs all the personal data provided in order to process it for the intended purpose, e.g. as a reinsurer receiving claims bordereaux it may not require the full personal details of claimants and can receive these on an anonymised or pseudonymised basis. Pseudonymised personal data is data which can no longer be attributed to a specific data subject

without additional information which is kept separately and securely e.g. an ID number on its own cannot identify the data subject without having the list of ID numbers with corresponding names, addresses and other data of each of the data subjects.

4. Accuracy.
The company must ensure that any personal data it holds is accurate and where necessary, up to date.

5. Storage Limitation.
Personal data must not be kept for longer than it is needed. The company should have a data retention and destruction policy to address this.

6. Integrity & Confidentiality
Personal data must be kept safe so that it doesn't get accidentally deleted or changed, or seen by someone who is not allowed to see it. The company's data protection and cyber security should address this.

7. Accountability.
The company must be able to evidence its accountability by showing how it takes responsibility for what it does with people's data. To do this the company must have appropriate data protection policies, procedures and controls in place which will include the documenting and monitoring of processes, staff training, cyber security measures and internal audits.

The board of a managed insurer should adopt data protection and cyber security policies and procedures of the Insurance Manager and will require the Compliance Officer to report to the board regularly on the operation of those policies and on any breaches.

The procedures will include a plan for dealing with data breaches, including a response to mitigate the impact of the breach, reporting to the ODPA, notifying the data subject and keeping a log of breaches.

The board may appoint a Data Protection Officer to implement and monitor its data protection governance framework but it is unlikely to be a legal requirement as the DP law only requires a DPO to be appointed where the company carries out large scale systematic monitoring of individuals (for example, online behaviour tracking) or large scale processing of special category data (i.e. racial or ethnic origin; political opinion; religious or philosophical belief; trade union membership; genetic data; biometric data; health data; sex life; criminal data) as part of its core activity.

Data controller and data processor

The DP Law distinguishes between data controllers and data processors.

Data controller: A person (individual or legal) who determines the purposes and means of the processing of any personal data.

Data processor: Any person, other than an employee of the data controller, who processes personal data on behalf of the data controller.

The legal obligations vary between data controllers and data processor. The data controller will be responsible for ensuring that any data processors it uses have adequate systems and controls in place to ensure compliance with the DP Law and the written contract with the data processor should place obligations on the data processor to comply.

Data audit

COMPLIANCE

It is important for the board to understand on what basis the company is handling data and ensure that policies and procedures for handling the data in compliance with the DP Law are in place and operating effectively.

At the introduction of the DP Law The board should commission the Insurance Manager to carry out a data audit and a Data Protection Impact Assessment (DPIA) which should be reviewed whenever there is a new or revised process involving personal data and updated to reflect any required changes.

The data audit identifies:

- what personal data the company has
- where the data has come from
- the valid legal reason for handling the data
- whether the company is acting as controller or processor
- where it is stored
- who has access to it

For insurers, personal data is likely to be handled as a data controller in respect of:

- underwriting information e.g. for health or life policies
- policyholder information
- claims data e.g. for health and liability claims
- CDD information on shareholders and directors.

A schematic may be produced showing the personal data flows, e.g. claims data may flow from the insured to the claims handler and then onto the company. A broker may also be involved in the data flow and the data may be forwarded to reinsurers by the broker.

The purpose of the DPIA is to ensure that all the data protection risks have been identified and addressed. The board will need to review all relationships it has with third parties where data is involved to ensure that it understands and is comfortable with the third party's controls and processes. It should also review the contracts with third parties and update them if necessary to reflect the DP Law.

15.5 CYBER SECURITY

Cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation from a failure of its IT systems. All licensed insurers are required to have robust policies, procedures and controls in place to identify, assess and manage cyber security risks on an ongoing basis.

The GFSC's Cyber Security Rules and Guidance, issued in 2021, set out the Rules that financial service businesses are required to follow in order to manage cyber risk, and provide guidance as to how a firm might satisfy the Rules. The board is responsible for ensuring that the Rules are followed and must be able to provide evidence that the Rules have been considered and implemented in accordance with the size, nature and complexity of the company's business.

For managed companies, the board will typically adopt the cyber security policies, procedures and controls of the Insurance Manager and will therefore need to gain assurances from the Insurance Manager that its cyber security framework complies with the Rules. The board would however be expected to have oversight of these services and would still be ultimately responsible for compliance with the Rules.

The board will also need to consider if there are any other service providers whose cyber risk may compromise the company (as well as individual directors who will also have access to the company's data) and gain the same assurances that their systems are compliant with the Rules. This may

include IT service providers and scheme administrators handling policyholder and other company data.

Most Insurance Managers have obtained Cyber Essentials Plus certification which will contribute significantly towards compliance with the Rules.

The Rules are based on **five core principles**:

Identify – the company's material assets and data and the associated cyber risks

Protect and Detect – ensure that appropriate policies and controls are in place to mitigate those risks and ensure business continuity in the event of a cyber security event. Controls will include cyber security software, timely IT system updates, encryption and dual factor authentication. Regular staff training will include awareness of e mail scams, phishing, passwords, physical security and internet use. Mechanisms in place to identify a cyber security event will include network monitoring tools.

Respond and Recover – a response and recovery plan should be in place to assess the impact of the event and respond appropriately. The plans should be tested regularly and improved as necessary. Secure back-ups of data will be a key part of the recovery plan.

Cyber security incidents must be notified to the GFSC.

15.6 ANNUAL SCHEDULE AND MEETING CHECKLIST

Annual regulatory deadlines for the company should be scheduled and reported on in the Compliance Report. These include:

Validation with the Company Registry
Insurance return including financial statements
Financial Crime Risk Return (for life insurers)
Tax return
Data protection registration
Holding of Annual General Meeting

The board will also agree an annual schedule which sets out what issues need to be considered at each (or a specific) Board or Committee meeting during the year. Some items will be considered at every board meeting but others will be scheduled to ensure that they are reviewed by the board at least annually at the appropriate time. This helps to ensure that all matters required to be addressed by the board are tabled at the appropriate board meeting and enables the Insurance Manager to draft the agenda and prepare the board papers for each meeting.

Standard items for consideration by the board at every meeting will typically include::

- Declaration of conflicts of interest
- Minutes of the last meeting and any written resolutions passed since then
- Matters arising from previous meetings
- Insurance Manager's report on underwriting performance
- Management accounts
- Forecasts
- Solvency
- Investment performance and banking arrangements
- Reinsurance security
- Compliance Report
- Any Other Business

Business which will be scheduled to be tabled for consideration at least annually include:

Module I Unit 15

COMPLIANCE

- Strategic objectives
- Business Plan
- Risk appetite and risk register
- Insurance strategy and renewals
- Reinsurance strategy
- Investment strategy
- Budget
- Accounting policies
- Reserving policies
- Annual Financial Statements
- Dividend policy
- Outsourced activities review
- Corporate Governance Code adherence review
- Tax return
- Management company and directors' fees

Module I Unit 15

COMPLIANCE

Self-test questions

. Answering these questions will remind the participant as to what has been learnt. Once completed, please check your answers against the relevant text.

1. What are the five core principals of the Cyber Rules?
2. Which insurers must submit an annual Financial Crime Risk Return to the GFSC?
3. Does an insurance company writing general insurance business need to be concerned about Money Laundering?
4. What distinguishes a Data Controller from a Data Processor?

Summary of learning outcomes
1. Describe the compliance requirements of a licensed insurer
2. Describe the role of the Compliance Officer
3. Explain the concept of three lines of defence
4. Describe the key components of a compliance report to the board
5. Explain the role of the insurance manager with regard to AML/CFT
6. State the seven data protection principles to be observed
7. State the five core principles of the Cyber Rules