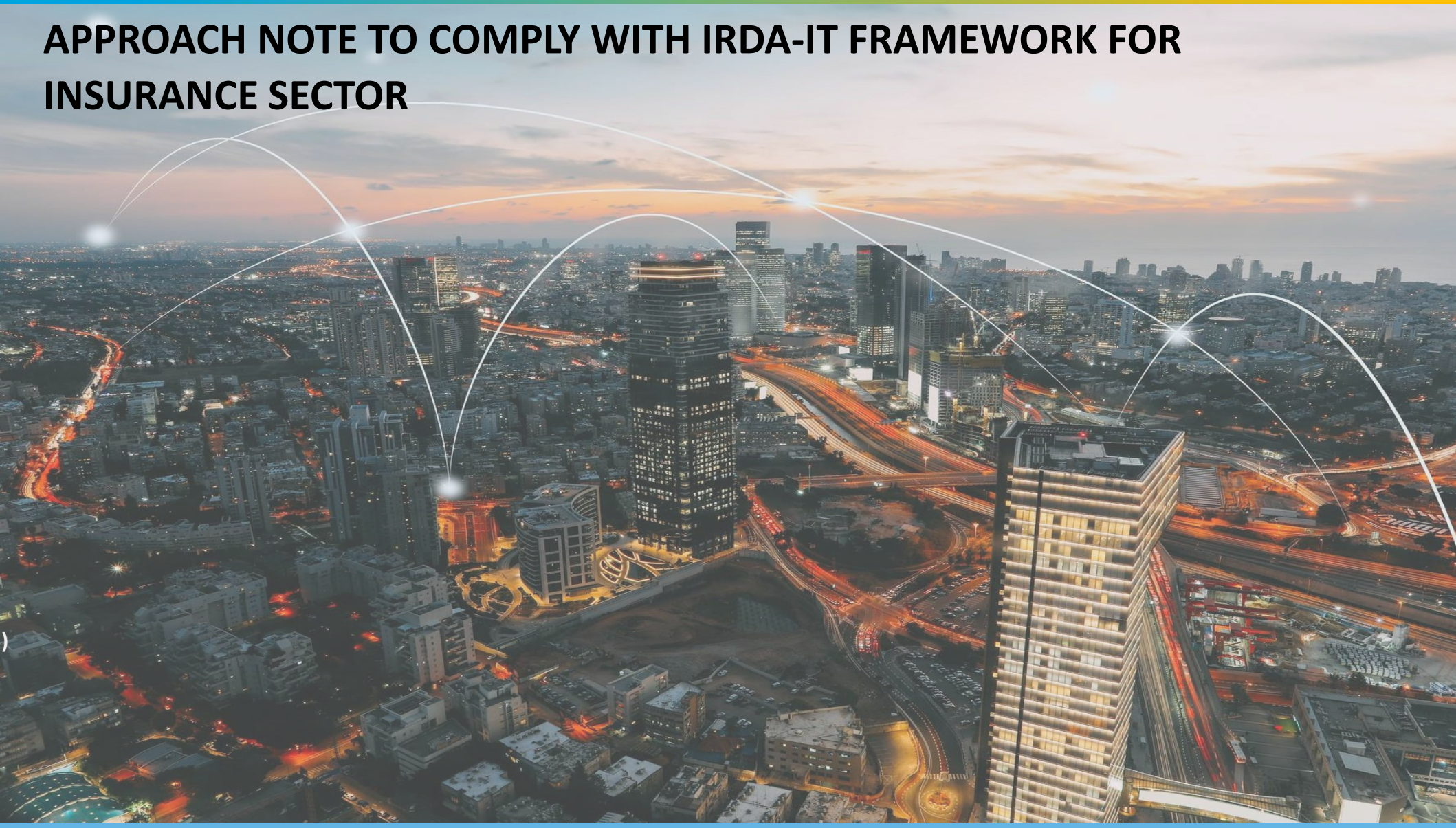
APPROACH NOTE TO COMPLY WITH IRDA-IT FRAMEWORK FOR INSURANCE SECTOR



ShineWing INDIA

Process, Risk and Technology Advisory

INFORMATION TECHNOLOGY FRAMEWORK
For Insurance Sector

Background

All insurers regardless of size, complexity, or lines of business, collect, store, and share with various third-parties (e.g., service providers, reinsurers etc.), substantial amounts of personal and confidential policyholder information, including in some instances sensitive health-related information. Insurance repositories, call centers, Common Service Centers etc. also have access to policyholders' data. . While Information sharing is essential for conducting the business operations, it is essential to ensure that adequate systems and procedures are in place for ensuing that there is no leakage of information and information is shared only on need-to-know basis.

Further, due to rapid development Information Technology, there are many challenges in maintaining confidentiality of information. The technology even though has many advantages, brings in risks associated with it like any other technology. With the fast growth of web based applications, cyber threat landscape has been growing and there is concern across all sectors. Cyber risks have grown and cyber criminals have become increasingly sophisticated. For insurers, cyber security incidents can harm the ability to conduct business, compromise the protection of personal and proprietary data, and undermine confidence in the sector. It is observed that the level of awareness of cyber threats and cyber security within the insurance sector, as well as supervisory approaches to combat the risks, appear to vary across organizations. Information obtained from regulated entities through cyber-crime may be used for financial gain through extortion, identity theft, misappropriation of intellectual property, or other criminal activities. Exposure of personal data can potentially result in severe harm for the affected policyholders, as well as reputational damage to insurance sector participants. Similarly, malicious cyber-attacks against an insurer's and Insurance Intermediaries' critical systems may impede its ability to conduct business.

Such security related issues have the potential to undermine public confidence and may lead to reputation risks to insurers. Hence, it is essential to ensure that a uniform framework for information and cyber security is implemented for insurers and an in-built governance mechanism is in place within the regulated entities in order to make sure that all such security related issues are addressed time to time.

Insurers who have not completed 3 years from the date of commencement of business are exempted from the requirement of a full-time person appointed as Chief Information Security Officer (CISO). However, the CISO responsibility may be taken care by any of the functionaries reporting to board. All other requirement stipulated in the guidelines document shall be applicable to these insurers. Reference to IRDA on it's circular ***IRDA/IT/GDL/MISC/082/04/2017*** has mentioned the Timelines of Implementation in which CISO must be appointed by 30th April'2017. Gap Analysis Report & Cyber Crisis Management plan must prepared by 30th June'2017. Information & Cyber Security policy must be finalized by 31st July'2017. IS and Cyber Assurance Programme in line with IS and Cyber policy must be formulated by 30thSept'2017. The first comprehensive information and Cyber Security assurance Audit must be completed by 31st March'2018.

Key Domains of the IRDA Circular & Guidelines

1. Timelines of Implementation
Various responsibilities of Chief Information Security Officer(CISO) may taken care by any of the functionaries reporting to Board. All other requirements stipulated in the guidelines document shall be applicable to these issuers.

2. Guidelines on Information & Cyber Security
To ensure a successful enterprise must effectively manage the union between business processes and information systems

3. ANNEXURE- A
Control checklist on implementation of information and Cyber Security Guidelines.

Vision and Objective

1. To ensure that a Board approved Information and Cyber Security policy is in place with all insurers.
2. To ensure that necessary implementation procedures are laid down by insurers for Information and Cyber Security related issues.
3. To ensure that insurers are adequately prepared to mitigate Information and cyber security related risks.
4. To ensure that an in-built governance mechanism is in place for effective implementation of Information and cyber security frame work.

How can We help?

Perform Current state assessment/ Gap Assessment	Using our inherent industry knowledge and ability to look at risks holistically, we can assist you in assessing the organizations current IT framework vis-à-vis requirements of IRDA mandated Information Technology framework. Our assessment program will also enable benchmarking the organizations measures to identify, protect, detect, respond, and recover from information security and cyber risks and threats to global frameworks.
Development of risk and controls framework to meet requirements	
Conducting training and awareness for employees and vendors	We can help you build your IT security and cybersecurity awareness and training program to enhance the risk culture in your organization.
Post assessment remediation assistance	Advising on remediation plans and program managing the actions to achieve the desired state of IT framework.

2. GUIDELINES ON INFORMATION AND CYBER SECURITY
For Insurance Sector

Background

IRDAI issued exposure draft containing the draft framework on 2nd March, 2017.Having considered the feedback received from the stakeholders to the Exposure draft, IRDAI now issues the "Guidelines on Information and Cyber Security for insurers" by exercising the power vested with the Authority under Sub-section (1) of Section 14 of IRDA Act,1999.

This guidelines are applicable to all insurers. In case of intermediaries and other regulated entries with whom the policyholder information is being shared, it would be the responsibility of the insurers to ensure that adequate mechanisms are put in place to ensure that the issues related to information and cyber security are addressed.
(Circular no. .IRDA/IT/GDL/MISC/082/04/2017)

Scope of Audit shall include assessments of the following areas :-

- Enterprise Security
- Information Assets Management
- Physical & Environmental Security
- Human resource security
- System acquisition, development and maintenance
- Information Security Risk Management
- Data, Application & Cyber Security
- Platform/ Infrastructure & Network Security
- Cryptography & Key Management
- Security Logging & Monitoring
- Incident Management
- Endpoint Security
- Cloud & Mobile Security
- Virtualization

Enterprise Security

1. Governance, Policy & standards, strategy
2. Establishment of governance framework
3. Information Security Training Goals
4. Identity and Access Management
5. Access control mechanisms , Privileged access , Authentication & password synchronization and Provisioning and de-provisioning.
6. Change Management & Implementation.
7. Vendor/Third party Risk Management
8. Business Continuity Plan

2. GUIDELINES ON INFORMATION AND CYBER SECURITY

For Insurance Sector

Information Security Management	To identify organizational assets, define appropriate protection and responsibilities. Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. The asset inventory should be accurate, up to date.
Physical & Environmental Security	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.
Human Resource Security	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
System acquisition, development and maintenance	To ensure that information security is an integral part of information systems across the system development life cycle.
Information Security Risk Management	To enable individuals who are responsible for target environments to identify key information risks and determine the controls required to keep those risks within acceptable limits. It Includes Managing Information Security Risk Assessment , Information Security Policy - Acceptable Use and Business Continuity & Disaster Recovery Framework.
Data Security	Organizations shall recognize that the efficient management of its data security is necessary to support its core functions, to comply with its statutory and regulatory obligations and to contribute to the effective overall management.
Application Security	To ensure that information security is an integral part of information systems across the entire lifecycle and also includes the requirements for information systems which provide services over public network.
Cyber Security	To raise awareness and provide guidelines to organizations for addressing cyber security and related risks to the insurance sector and the mitigation of such risks.
Platform/Infrastructure Security	Organization's IT infrastructure including servers, applications, and network and security devices shall be configured to ensure security, reliability and stability.

2. GUIDELINES ON INFORMATION AND CYBER SECURITY

For Insurance Sector

Network Security	The information transmitted across the Organization through its network shall be protected by deploying adequate network security controls.
Cryptography & Key Management	Organization shall protect the confidentiality, authenticity and integrity of information by cryptographic means wherever necessary. The level of protection applied using cryptographic keys shall be commensurate with the sensitivity and frequency of use of the information along with the environment where it resides/used. .
Security Logging & Monitoring	Organizations shall establish logging and monitoring capabilities to detect security events in timely manner.
Incident Management	To ensure information security and cyber security events and weaknesses associated with the information systems are communicated and corrective actions are taken in a timely manner.
Endpoint Security	Policy, Procedures & Guidelines: Policy, Standards, Procedures and Guidelines shall be developed to address the threats to endpoints in information system infrastructure and to prevent unauthorized access to endpoints.
Virtualization	To ensure protection of information during use of virtual environment within the IT infrastructure of the company.
Cloud Security	To ensure that information processed, transmitted and stored on the cloud architecture is secure.
Virtualization	To ensure the security of information assets while tele-working and using the mobile devices by implementation of appropriate security measures to manage the risks associated with the usage of mobile computing devices and communication facilities.

3. ANNEXURE- A
For Insurance Sector

Background

The commencement of any audit is with the review of the background of the organization to understand its activities and the impact of IT on these activities. Along with the nature of organization, the audit party would be specifically interested in the background of IT systems in use in the organization.

Multiple IT systems may be in use in an organization. The auditor may not be interested in auditing all the IT applications in an organization. The nature, extent and scope of the IT audit and the resources committed for the job are dependent upon the subjective assessment of the risk parameters or in other words, criticality of the application. The process of establishing the criticality of a system is subjective.

CONTROL CHECKLIST ON IMPLEMENTATION OF INFORMATION AND CYBER SECURITY GUIDELINES

Information Security	• The Organization should have a risk management program to undertake information security risk assessment for target environments (e.g. critical business environments, business processes, business applications, computer systems and networks) on a periodic basis. • Information security function exists distinct from IT function with dedicated responsibility of defining and monitoring implementation of information security policies and controls.
Human Resource Security	• A code of conduct may be used to state the employee's or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. • Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills.
Assets Management	• Ensure that assets are inventoried • Ownership of the asset should be assigned . • Sign off must be obtained from employees, contractors and third party for the acceptable usage policy • Ensure proper handling when the asset is deleted or destroyed. • Define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies

3. ANNEXURE- A
For Insurance Sector

Access Control	• User Access Management -User Registration & Privilege Management. • Password Management system • User Access Management -Review of user access rights. • Role-based and least privilege access mechanisms must be in-built into systems to enable authorized access as per job roles.
Cryptography	• There must be Policy on use of cryptographic controls. • All passwords rendered must be unreadable during transmission and storage on all system components using strong cryptography for Portals.
Physical & Environmental Controls	• There must be sufficient controls in place for physical protection against damage from fire, earthquake, explosion, civil unrest and other forms of natural or man-made disaster. • Fire extinguishers installed at easily visible and accessible locations. They must be adequate in number for the area to be covered. • Air conditioning systems shall be implemented to ensure that the operational environmental conforms to the equipment manufacturer's specifications.
Operations Security	• Operating procedures are documented and made available to all users who need it. • There must be procedure for decommissioning of applications, systems, databases or environments etc. • Backup media stored in fire resistant cabinet in line with the OEM specifications and accessible to only authorized personnel. Change management process must include planning and testing of changes
Communication Security	• Controls were implemented to ensure the security of the information in networks, and the protection of the connected services from threats, such as unauthorized access. • Security mechanisms, service levels and management requirements of all network services identified and included in network services agreements
System Acquisitions, Development & Maintenance	• Security requirements for new information systems and enhancement to existing information system specify the requirements at time of implementation/ design for security controls. • Testing of security functionality are carried out during development. • Supervise and monitor the activity of out sourced system development.

3. ANNEXURE- A
For Insurance Sector

Information Security in Supplier Relationships	• Processes and procedures established for information security requirements for each type of vendor and type of access based on the organization's business needs and the risk profile. • The supplier agreements must include legal and regulatory requirements, data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met
Information System Incident Management	• Incident management policy and procedures must define processes to be followed for incidents related to all systems including applications and infrastructure capturing the version history and approval history. • exists a procedure that ensures all employees of information systems and services are required to note and report any observed or suspected security weakness in the system or services. • Management must have a defined and documented procedures for identifying security related incidents by monitoring logs generated by various IT assets
Compliance with Legal Requirements	• Controls such as: publishing intellectual property rights compliance policy, procedures for acquiring software, policy awareness, maintaining proof of ownership, complying with software terms and conditions are considered. • All relevant statutory, regulatory, contractual requirements and organizational approach to meet the requirements were explicitly defined and documented for each information system and organization.
Business Continuity Management	• Internal procedures are developed and followed when collecting and presenting evidence for the purpose of disciplinary action within the organization. • IT Disaster Recovery Management (IT DR) framework to improve the resiliency of the organization and ensure availability of the IT systems supporting the business operations. • Business continuity plans are tested regularly to ensure that they are up to date and effective. • Third party must evaluate DR Program in the past 12 months • Incident response personnel identified with necessary responsibility, authority & competence to manage an incident & the same must communicated to the concerned personnel. • Detailed recovery procedures (applications, Infrastructure components) must be documented for an effective recovery of the business applications.

Process & Risk | Technology | Assurance | Tax | Transactions | Advisory

Gurugram

I Floor, AIHP Palms, Plot no.
242 – 243, Udyog Vihar,
Phase – IV, Gurugram,
Haryana - 122015

Mumbai

203, The Summit,
Vile Parle, Western Express
Highway, Mumbai

Hyderabad

4th Floor, Tower B, Win Win
Towers, JNTU - Hitech City Main
Road, Khanamet, Madhapur,
Hyderabad - 500 081

Pune

124, Sohrab Hall,
Sasoon Road,
Opp. Jehangir Hospital,
Pune 411001

Chandigarh

3020, Sector 46-C
Chandigarh, U. T

Amritsar

23, Anand Avenue,
Maqbool Road
Punjab

Chennai

B-403, Prince Garden,
No. 40, Thambusamy Road,
Kilpauk,
Chennai – 600 010

www.sw-india.com