**SECURITY STANDARDS**

As a regulated entity, Ardonagh is required to ensure that its suppliers, and their supply chain have appropriate risk management procedures and systems in place. This Security Standards Framework sets out Ardonagh’s minimum security standards. The Supplier shall also have, maintain, regularly update and adhere to its own security policies and standards which comply with the requirements below.

Pursuant to the agreement between Ardonagh and the Supplier, the Supplier agreed to comply with Ardonagh’s policies and requirements and this Security Standards Framework is deemed to form part of the agreement.

|  |
| --- |
| **3rd Party Security Risk Management Business Standard**  |
| **CSRM1. Security Governance** | 1.1 A documented governance mechanism for cyber security must be established, approved, owned and monitored by a relevant governing body in accordance with recognised Good Industry Practice for information security, cyber security and cryptography (by way of example, aligned to the standards and/or guidance of ISF, NIST, ISO27001 or the Bank of England and such other similar standards and guidelines as may be created from time to time) (“**Good Security Practice**”).1.2 The governance mechanisms must clearly define the objectives of the governing body, which must align with the business strategy, delivering stakeholder value and providing assurance that information risks are being addressed.1.3 The governing body is responsible for the oversight and challenge of delivery against a ‘Cyber Security Policy’ and its strategic and operational implementation in accordance with a recognised security risk management framework implemented pursuant to Good Security Practice. It must meet regularly to review and challenge relevant management information and proposals in order to make effective and informed decisions in relation to security risk management. 1.4 A documented information security governance mechanism that details information security controls aligned with relevant industry frameworks and where required derived from regulatory and legal requirements and contracts must be approved by the governing body, maintained and implemented.1.5 Methods of assessing and meeting security requirements are overseen by the governing body and must be defined and agreed by IT teams and applied consistently. |
| **CSRM2. Security Direction**  | 2.1 A high-level working group, management committee or equivalent body must be established, to provide, oversee and co-ordinate operational security activity. 2.2 A Chief Information Security Officer (CISO) or equivalent must be appointed by/and or agreed by the executive management, with overall responsibility for the delivering a Cyber Security Policy and associated business standards and minimum requirements using a risk-based approach. 2.3 The CISO will chair any relevant management forums.  |
| **CSRM3. Security Policy Management**  | 3.1 A documented ‘Cyber Security Strategy’, that is readily accessible, must be maintained, reviewed and approved by the relevant forum on at least an annual basis. 3.2 The Cyber Security Strategy must clearly set out:3.2.1 How cyber security activities will be aligned with strategic objectives and risk appetite; and3.2.2 How cyber and information security risk reduction will be achieved, how to protect the interests of stakeholders and consider business and cyber security context. |
| **CSRM4. IT devices and systems** | 4.1 A detailed ‘Acceptable Use’ document must be in place which is attested to by all staff.  |
| **CSRM5. Information Security Function** | 5.1 A specialist information security function, led by a CISO or equivalent with adequate senior management support and resources, must be established to promote: a Cyber Security Policy and associated business standards and minimum requirements; security governance, risk and controls oversight and SME advice throughout the business; and information security awareness and culture across the business. |
| **CSRM6. Information Security Risk Assessment**  | 6.1 A documented information risk methodology must be used to perform information security risk assessments for each IT environment and escalate in accordance with documented approval matrix on a quarterly basis and when environments, including those under development, undergo major or significant change (e.g. new or altered critical business environments, processes and applications and supporting technical infrastructure) in accordance with a recognised security risk management framework implemented pursuant to Good Security Practice. 6.2 Appropriate information security risk assessments must also be sought and/or undertaken with regards to new and existing third party relationships, change projects and mergers and acquisitions. 6.3 Information security risk reports must provide accountable executive management with an accurate, comprehensive and coherent view of information security risk across the business, and must be aligned with, and support, the requirements of the enterprise and operational risk management frameworks. |
| **CSRM7. Security Audit Management** | 7.1 Independent, regular security audits must be conducted on target environments (e.g. critical business environments, processes, applications and supporting technical infrastructure) to provide owners and executive management with effective oversight of their implementations, the relevant security controls environment and their cyber security risk assessment (CSRM6). 7.2 Audits methodologies must be conducted in accordance with a recognised security risk management framework implemented pursuant to Good Security Practice. |
| **CSRM8. Security Monitoring and Reporting** | 8.1 The status of cyber security threats, risks and controls across the business must be monitored by IT and security teams (and where appropriate other control owners based in other functions i.e. HR) and reported on a regular basis through appropriate reporting structures to key decision-makers and accountable senior management.8.2 The business must, in a timely manner, collectively monitor:* + 1. Progress and performance of plans to deliver any strategy and documented objectives;
		2. Remediation plan progress and identification of areas for further improvement;
		3. Performance of cyber risks and controls, using suitable assessment methods, key performance indicators (KPIs) and key risk indicators (KRIs), which are tested and confirmed by relevant audiences (e.g. phishing tests);
		4. Mandatory training completion rates; and
		5. Remediation of any significant risks, issues or actions arising from risk and control assessments, audits and/or incidents, including comparison of sources to identify and manage trends and patterns.
 |
| **CSRM9. Security Awareness and Education** | 9.1 The business must maintain an ongoing and adequate security awareness programme of activities to promote and embed expected security knowledge and behaviour in all individuals who have access to business information and systems in accordance with a recognised security risk management framework implemented pursuant to Good Security Practice. |

|  |
| --- |
| **3rd Party Security Operations Business Standard** |
| **CSO1. Security Solutions**  | * 1. A documented security architecture framework, approved by the CISO and relevant IT teams, must be designed and its principles implemented by all relevant teams.
	2. Adequate processes for identity and access management (IAM) must be designed and implemented, with additional controls for high-risk systems.

1.3 User entitlement reviews and user access recertification must be conducted on all required applications and users at the required cadence.  |
| **CSO2. Data Risk Solutions** | * 1. Business critical systems and network boundaries between any untrusted and trusted network segments must be protected by adequate intrusion detection systems and supporting processes to monitor and respond to alerts.
	2. Data Loss Prevention (DLP) technical controls must be implemented using a risk-based approach on critical systems that process, store or transmit personal or confidential information, with processes to monitor and respond to system alerts. This can include the implementation of specific DLP technical solutions and tooling, alongside existing DLP mechanisms and controls embedded within existing technology solutions, where present. e.g. MS E5 licences.
	3. All sensitive information that needs to be protected from unauthorised disclosure and/or unauthorised access must be identified to the relevant IT team, recorded in a data asset inventory by that IT team, and all business information (‘Data’) must be appropriately labelled and classified in accordance with Good Security Practice.
 |
| **CSO3. Cryptography**  | 3.1 Cryptographic solutions and technical controls must be selected and implemented that protect confidentiality of information and assess information risks, that are approved by authorised persons and supported by adequate documented processes.3.2 Public Key Infrastructure, which includes the issuing and review of certificates, must operate documented processes in accordance with Good Security Practice.  |
| **CSO4. Cyber Security Resilience**  | 4.1 Documented adequate vulnerability management processes, controls, solutions and procedures must be in place for:4.1.1 Identifying, regularly scanning, risk assessing, prioritising, remediating and reporting technical vulnerabilities in business applications and systems;4.1.2 Effectively identifying, testing, deploying and recording patches (patch management) in a timely manner; and4.1.3 Emergency fixes.4.2 A threat intelligence capability must be developed and operated that has processes to produce or obtain adequate threat intelligence on a regular basis for security SME review and action.4.3 The effectiveness of security controls and cyber event/incident response and recovery capabilities must be adequately tested, and where required, enhanced by simulating attacks through various means on at least an annual basis.4.4 Regular management information and proposals on existing threats, vulnerabilities, the effectiveness of existing controls, residual risk and any planned improvements must be reported to the relevant accountable and responsible individuals) and/or relevant governance forums within agreed timeframes.  |
| **CSO5. Security Incident Management**  | 5.1 An adequate documented approach and associated minimum process requirements must be designed, documented and implemented for information and cyber security incident management and response. 5.2 Documented operational processes, resource plans and adequate skilled resources must be in place at a local segment level to support any incident management framework and minimum requirements.  |
| **CSO6. Malware Defence**  | 6.1 Monitoring and response procedures must be in place for malware related threat intelligence. 6.2 Malware protection software must be deployed, configured and monitored (all in accordance with Good Security Practice) on all desktops, laptops, servers (both physical and virtual), other endpoints (where appropriate), firewalls and email gateways.  |
| **SOC7.****Systems Security Information and Event Management**  | 7.1 Important security-related system information and events must be defined and recorded in system logs that are suitably protected, retained for at least 13 months and available in a reasonable timescale when needed. 7.2 All logs must be synchronised with a single master time source on each IT estate.7.3 A security event management process including logging, monitoring, alerting and response must be designed, documented and implemented by IT and Security teams in accordance with Good Security Practice to identify and alert, triage, investigate, trigger security incident managed and help respond to security-related events. 7.4 The security event management process must, include all business-critical systems and be integrated with organisational incident management, business continuity and crisis management processes. |

|  |
| --- |
| **3rd Party IT Security Management - Networks and Systems Standard** |
| **CITSM1. Business Applications** | 1.1 All information system assets (to include all software, hardware and informational assets held on systems) must be documented in a register, with the appropriate minimum information, which is reviewed and updated by the appropriate business manager.1.2 All business applications must use technical measures to: 1.2.1 Protect against unauthorised access and/or disclosure of Confidential Information;1.2.2 Prevent accidental corruption or deliberate manipulation, ensure availability and resiliency;1.2.3 Implement secure design and coding practices; and 1.2.4 Prevent hijacking, cloning and/or interception.  |
| **CITSM2.Information Validation** | 2.1 Information validation processes must be implemented for data integrity, data inputs and data outputs, which are used by the relevant project teams to check validity, accuracy, completeness and timeliness (in accordance with the level of risk).  |
| **CITSM3.End User Developed Applications -EUDAs**  | 3.1 All EUDAs are developed and designed in accordance with a documented methodology, testing plan and ownership requirements, which are reviewed and signed off by authorised individuals. 3.2 Details of all EUDAs must be maintained in an inventory with the appropriate minimum information. 3.3 Risks associated with unauthorised access and modification to critical spreadsheets, databases and other EUDAs including the information contained within them are documented and managed or mitigated using technical controls. 3.4 The relevant Senior Manager or Certified Person must approve the use and creation of EUDAs prior to them being used.  |
| **CITSM4.System Management** | 4.1 Systems (e.g. computer and network installations, server configurations) must be designed using sound security architecture principles, including appropriate segmentation. Systems must, by design and function:4.1.1 Accommodate all current and predicted capacities and workloads; 4.1.2 Have resilient design that is appropriate to the system’s BIA rating; and 4.1.3 Use appropriate network and system component segregation. 4.2 Standard builds must be in place and adhered to, to ensure that all systems are suitably hardened to protect against malfunction, cyber-attack, unauthorised disclosure, corruption and loss. 4.3 Systems must be deployed consistently and regularly maintained. They must be appropriately controlled, including but not limited to: 4.3.1 Regular vulnerability scanning, vulnerability remediation and patching; 4.3.2 Design and build standards for physical servers, virtual servers and network storage systems that are commensurate with the sensitivity of data to be processed; and 4.3.3 Monitoring and regular security testing.  |
| **CITSM5.System Maintenance** | 5.1 Each company must identify and document who is responsible for the oversight and management of adequate system maintenance and service level agreements for computer and network services that support critical business applications. 5.2 Adequate back-up (including resilient backups) systems and processes must be in place, in accordance with relevant and up-to-date business impact assessments, business continuity management requirements and IT disaster recovery plans, with all back-ups adequately protected and stored in secure, appropriately distanced and/or ‘offline’ locations. 5.3 IT systems and backups that support critical business services must have their technical recovery capability regularly (at least annually) tested.  |
| **CITSM6.Network Management** | 6.1 Network accountabilities must be clearly documented, with networks and network device configurations:6.1.1 Understood and clearly documented;6.1.2 Configured to prevent unauthorised access or incorrect updates; and 6.1.3 Supported by appropriate technical and operational processes including documented network diagrams, configuration information, network security architecture, details on segmentation, inventories and labelling. 6.2 Wireless access to networks must have adequate additional technical controls and oversight, and documented inventory of access points, encryption of all connections network segregation and the use of VPNs.6.3 External (remote) network connections must be configured and protected to prevent unauthorised access and protect data in transit. They must:6.3.1 Use multi-factor authentication; 6.3.2 Use dedicated remote access servers;6.3.3 Use strong encryption and authentication methods in accordance with Good Security Practice;6.3.4 Subject to documented executive approval.6.4 Network traffic must be routed through a firewall at all network entry and exits points. Firewall technologies and their configurations must be regularly maintained and reviewed at least annually.  |
| **CITSM7.Electronic Communications** | 7.1 Communication systems (e.g. email, collaboration platforms and voice communication platforms) must operate:* + 1. On resilient infrastructure;
		2. Technical security controls that prevent common threats (e.g. email spoofing) and protective measures (e.g. opportunistic TLS is enabled);
		3. Security requirements for collaboration systems in accordance with Good Security Practice; and

7.1.4 Technology specific controls that are commensurate with the risk.  |
| **CITSM8.Mobile Computing** | 8.1 Mobile devices (e.g. laptops, tablets and smartphones) must have the following security controls implemented:8.1.1 Authentication controls to gain access to the device;8.1.2 Automatic screen locking after periods of inactivity;8.1.3 Restrictions of wireless connectivity; 8.1.4 Physical security protections (e.g. cable locks); and8.1.5 Standard hardened build configurations. 8.2 Mobile devices must be controlled by centralised systems that provide Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM) functionalities and must be technically configured to protect sensitive information processed and stored on them including, but not limited to, the use of VPNs. 8.3 The use of personally owned mobile devices must:8.3.1 Be approved by management in advance;8.3.2 Be supported by enforceable usage agreements; and8.3.3 Have adequate technical controls operating on the device. 8.4 Portable storage devices must be technically blocked by default. Process and technical controls must be in place to authorise, protect and control any exceptions. 8.5 Remote workers must be provided with appropriate equipment and technical controls to enable them to work securely. Additional controls must be given to workers who travel to and from (or through) high risk countries. |

|  |  |
| --- | --- |
| **CITSM9.Access Management** | 9.1 Technology controls must be in operation that authorise user access and restrict access to business applications, mobile devices, systems and networks to authorised individuals for specific business purposes.9.2 All access privileges are granted based on user roles, must be approved and a record kept of all access granted. 9.3 Suitable additional controls must be documented, implemented and reviewed (at least annually) for IT administrative privileges. In addition: 9.3.1 Service accounts must not support interactive logons; 9.3.2 Domain admin accounts must be minimised; 9.3.3 There must be no more than 3 Enterprise admins accounts; and 9.3.4 The KRBTGT account must be reset regularly (at least annually). 9.4 Two-factor or Multi-factor (2FA or MFA) must be in place for any non-console remote access to systems, and all exceptions are subject to documented risk acceptance. 9.5 Access and authentication controls must be implemented, and protected by encryption requirements, in accordance with Good Security Practice.9.6 Documented process for account management must be implemented in accordance with Good Security Practice.9.7 The selection of systems must be evaluated and documented.  |
| **CITSM10.Customer Access (including key business partners)**  | 10.1 Business applications that allow access to customers or key business partners (e.g. Insurers) must be protected by appropriate additional controls including:10.1 Records of authorised customer connections and requirements;10.2 Expert security review;10.3 Security guidance for customer users;10.4 Suitable contracts; and10.5 Technical access security controls based on the sensitivity of data processed. |
| **CITSM11.System Development Management** | 11.1 Secure systems development methodologies and practices must be documented, communicated and consistently implemented for all systems development activities with regular IT management oversight. 11.2 Controls must be in place to ensure appropriate access to development and test environments, segregation of duties between environments and to protect production / non-production environments, source code and test data. 11.3 Systems development must be subject to review and sign-off by project stakeholders at key points through the project to gain assurance that the project is adhering to design and build methodologies, security, functional and non-functional requirements. 11.4 There must be process(es) for tracking and remediating security deficiencies found development projects in a timely fashion. 11.5 The design process of any new systems under development must consider, functional, non-functional and appropriate security and regulatory requirements and have a security SME and solution architect review of the documented designs. 11.5 Third party software must be appropriately documented, owned and managed.11.6 System build activities must adhere to appropriate secure build practices, testing and approval processes. 11.7 All implementation and post implementation activities must be completed and verified before the project is closed. |
| **CITSM12.Change Management**  | 12.1 A process must be established and embedded to formally govern, document and approve all changes to IT technical environments. 12.2 There must be clear criteria for submitting, reviewing, approving and testing changes including:12.2.1 Documenting installation processes;12.2.2 Operational processes; 12.2.3 Post implementation checks;12.2.4 Success criteria; and12.2.5 Lessons learned. 12.3 The change management process must provide a clear audit trail of all change requests including roll-back plans and sign-off from all key stakeholders in each change.  |
| **CITSM13.****Systems Lifecyle**  | 13.1 IT hardware must be managed appropriately through its lifecycle, including but not limited to:13.1.1 Security review of the system and supplier due diligence prior to acquisition; 13.1.2 Asset records management that records all key information; 13.1.3 Management processes for devices within operational lifespan and to identify and replace equipment before it reaches the end of its working life; and13.1.4 Timely documented secure disposal and destruction practices for all equipment following retirement.  |
| **CITSM14.Office Equipment** | 14.1 Office equipment must be securely managed and maintained by:14.1.1 Assigning ownership;14.1.2 Implementing access controls (for both the hardware and the information it processes); and14.1.3 The application of additional technical security controls for high risk information in accordance with Good Security Practice.  |
| **CITSM15. Systems Performance & Monitoring** | 15.1 There must be operational processes to monitor and report on the performance of business applications, infrastructure, networks and other systems/computing devices against agreed performance levels. 15.2 Monitoring must take place in accordance with the details set out in a recognised security risk management framework implemented pursuant to Good Security Practice. |
| **CITSM16.Business Continuity (and Operational Resiliency)** | 16.1 Critical business applications and underlying infrastructure must be designed for high availability and resiliency, including support from alternative or duplicate systems or system components.16.2 Resiliency and technical recover plans must:16.2.1 Identify and document all critical applications and infrastructure; 16.2.2 Protect that those systems in accordance with their risk; 16.2.3 Produce detailed runbooks and realistic recovery scenarios;16.2.4 Be tested on at least an annual basis; and16.2.5 Reviewed regularly and incorporate lessons learned from testing.  |
| **CITSM17.Specialist Training**  | 17.1 IT system owners and IT technical specialists must be equipped with the necessary skills, knowledge, tools, resources and authority to fulfil their responsibilities. This should be achieved through system management procedures and specialist training programmes, as well as being appropriately managed and overseen in day-to-day operations to minimize the risk of theft, fraud, error and/or malicious or accidental access and/or changes to information.  |

|  |
| --- |
| **3rd Party Cyber Security Policy** |
| * 1. **Security Risk Management**
 | * + 1. Security Governance - Establish, maintain and monitor information security governance mechanisms, which support the appropriate governance structures and accountable senior management.
		2. Security Direction - Establish a high-level management committee (or equivalent) and a Chief Information Security Officer (CISO) (or equivalent) to oversee and co-ordinate security activity across the business.
		3. Security Strategy - Support information security governance by creating an information security strategy and implementing an information security assurance programme, which are aligned with the business and IT strategies, objectives and risk appetites.
		4. Security Policy Management - Develop a comprehensive, approved information security policy framework (including supporting policies, standards and/or procedures, such as Acceptable Use) and communicate it to all individuals with access to business information and systems.
		5. Information Security Function - Establish a specialist information security function led by a sufficiently senior manager (e.g. a CISO) who is assigned adequate authority and resources to run information security-related operations and projects.
		6. Information Security Risk Assessment - Adopt and apply an information security risk assessment methodology to critical business activities (e.g. projects, acquisitions) that includes activities such as scoping, business impact assessment, threat profiling, vulnerability assessment, risk evaluation and risk treatment, and that covers confidentiality, integrity and availability requirements. Use this methodology in a rigorous and consistent manner to conduct regular information risk assessments for target environments (e.g. critical business environments, processes, applications (including those under development) and supporting technical infrastructure).
		7. Security Audit Management - Conduct thorough independent and regular audits of the security status of target environments (e.g. critical business environments, processes, applications and supporting technical infrastructure). Audits must be conducted using a consistent methodology that includes planning, fieldwork, and reporting phases in addition to ongoing monitoring.
		8. Security Monitoring and Reporting - Monitor information risks and regularly assess and test related controls; review compliance with the security-related elements of legal, regulatory and contractual requirements; and assess the overall information security condition of the business on a regular basis; reporting the results to specific audiences, such as executive management.
		9. Security Awareness and Education - Maintain a comprehensive ongoing security awareness programme, including regular awareness messages and periodic training, to promote and embed expected security behaviour in all individuals who have access to the business information and systems.
 |
| **3.2 IT Security Management - Networks and Systems** | * + 1. Business Applications - Manage, document and incorporate security measures into business applications, including specialised controls for web browser-based applications.
		2. Information Validation - Incorporate integrity measures into business applications to protect the quality of information when it is input to, processed by and output from these applications.
		3. End User Developed Applications (EUDA) - Develop critical EUDA, such as spreadsheets and databases, in accordance with an approved development methodology.
		4. System Management - Design systems (e.g. computer and network installations, server configurations) to cope with current and predicted workloads and configure them in a consistent and accurate manner to protect them and the information they process and store against malfunction; cyber-attack; unauthorised disclosure; corruption; and loss.
		5. System Maintenance - Manage the security of systems by performing regular backups (which must include offline backups) of essential information and software, applying a rigorous and controlled change management processes and monitoring performance against agreed service level agreements.
		6. Network Management - Design physical, wireless and voice networks to be reliable and resilient; prevent unauthorised access; encrypt all wireless connections; and detect suspicious traffic. Configure network devices (including routers, firewalls, switches and wireless access points) to prevent unauthorised or incorrect updates, including securing remote maintenance practices.
		7. Electronic Communications - Protect electronic communication systems (e.g. email, collaboration platforms and voice communication platforms) by setting security policies for their use; configuring security settings; and hardening the supporting technical infrastructure.
		8. Mobile Computing - Mobile devices (including laptops, tablets and smartphones) and the information they handle must be protected against loss, theft and unauthorized disclosure.
		9. Access Management - Restrict access to business applications, mobile devices, systems and networks to authorised individuals for specific business purposes on a ‘needs-to-have’ basis in line with role and ensure robust operational processes and controls in relation to identity and access management. Restrict and appropriately control any Domain or Local Administrator accesses and accounts with any elevated privileges.
		10. Customer Access - Protect business applications that provide customer access by performing information risk assessments to determine information security requirements and implementing security arrangements and technical security controls (e.g. connectivity controls) that are supported by agreed, approved contracts.
1. System Development Management - Establish a structured system development methodology that applies to all types of business IT systems (including applications and related technical infrastructure) in accordance with Good Security Practice and by incorporating information security during each stage of the lifecycle.
	* 1. Change Management – All changes (including emergency changes) to IT technical environments must be adequately governed, controlled, documented and approved.
		2. Systems Lifecyle Management – Protect IT hardware assets, including systems and network devices and specialist equipment, throughout their lifecycle addressing the information security requirements for their acquisition (e.g. purchase or lease), maintenance and disposal.
		3. Office Equipment- Protect physical technology assets used in the office (e.g. network printers and multifunction devices) addressing the information security requirements for their ownership, authentication and location.
		4. Systems Performance and Monitoring – Business applications, infrastructure, networks and other systems/computing devices must have their performance monitored against agreed performance levels and intervals, with supporting reporting and remediation processes.
2. Business Continuity (and Operational Resiliency) – Establish resilient (high availability) IT systems to support critical business processes in line with Business Continuity plans and latest business impact analysis, including duplicate or back-up systems and technical recovery planning and sample testing on at least an annual basis.
	* 1. Specialist Training - IT system owners, IT technical specialists and Information / Cyber Security staff must have the necessary skills, tools, resources and authority to fulfil their roles and responsibilities.
 |
| **3.3 Security Operations** | **3.3.1** **Security Solutions** - Build a sound technical security infrastructure, applying security architecture principles and integrating technical security solutions across the technology estate, which includes (but not limited to) malware protection and identity and access management. **3.3.2** **Data Risk Solutions** – Technical and operations solutions must be deployed to protect data risks including but not limited to intrusion detection and prevention, data loss (leakage) prevention, data discovery and data asset management.**3.3.3** **Cryptography** - Deploy approved cryptographic solutions (e.g. endpoint encryption, public key infrastructure and digital signatures) to help protect the confidentiality of information, determine if critical information has been altered, provide strong authentication and support non-repudiation.**3.3.4** **Cyber Security Resilience** - Manage threats and vulnerabilities associated with those critical business applications, systems and networks that underpin critical business operations, processes and services. **3.3.5** **Security Incident Management** - Establish a comprehensive and approved information security incident management approach, which is supported by a process for the analysis, containment, eradication, response, recovery and post incident review of information security incidents. It should also be appropriately integrated with wider Business Continuity Management and Crisis Management frameworks and processes.**3.3.6** **Malware Defence** – Malware protection systems must be implemented with supporting process to identify threats and maintain updates. **3.3.7** **Systems Security Event Management** – Establish a security event logging and monitoring process to identify, triage, investigate and help respond to security-related events that is supported by suitable tools and processes and applies to all important IT systems. |