Information Security Management Programme

Contact maintains an Information Security Management Programme designed to protect information, technology systems and operational environments from evolving cyber and information security threats.

The programme supports Contact's ability to operate safely, securely and reliably while enabling technology change, digital services, operational resilience and strategic delivery.

Our programme is risk-based and includes governance, risk management, secure delivery, vulnerability management, security monitoring, incident management, awareness and education, business continuity and resilience, third-party security, assurance and continuous improvement.

Governance and accountability

Information security is governed through Contact's broader risk management framework and technology governance. The Board maintains oversight of material cyber and information security risks through the Audit and Risk Committee, supported by regular reporting on risk appetite, programme delivery, incidents, assurance activity and improvement priorities. Executive accountability sits within the technology team.

Security responsibilities are supported by policies, standards, governance forums and risk management processes. These help define expectations for people, technology teams, suppliers and business owners who use, manage or protect Contact information and systems.

Risk management and secure delivery

Contact applies a risk-based approach to information security. Security risks are identified, assessed, treated and monitored in line with Contact's risk management framework and business priorities.

Security considerations are included in technology strategy, architecture, solution delivery, supplier engagement and operational change so that risks are considered early and managed throughout the technology lifecycle.

This helps Contact support secure technology delivery, maintain stable and secure systems and reduce the likelihood and impact of cyber events affecting customers, information, operations or business services.

Vulnerability management and security testing

Contact maintains activities to identify, assess, prioritise and remediate vulnerabilities across technology environments. This includes vulnerability management, security testing, prioritised remediation and targeted review of systems and services. Risk-based prioritisation is used to focus effort on vulnerabilities and control gaps with the greatest potential impact if exploited.

Security testing and assessment activities help validate control effectiveness, identify weaknesses and inform remediation roadmaps and future investment.

Security monitoring and incident management

Contact maintains security monitoring and incident management processes to support detection, escalation, assessment and response to suspected cyber and information security events.

Employees, contractors and service providers are expected to report suspected information security incidents, vulnerabilities or suspicious activity through established internal reporting channels.

Incident response activity is supported by escalation processes, investigation, containment, communication, lessons learned and ongoing improvement. Where appropriate, material issues are escalated through governance and risk management channels.

Business continuity and operational resilience

Contact recognises that information security and operational resilience are closely connected.

The Information Security Management Programme supports business continuity and technology resilience by helping protect critical systems, maintain recovery capability and reduce the likelihood and impact of cyber events that could affect business operations.

Security and resilience activities include consideration of disaster recovery, business continuity requirements, incident response, technology asset management and assurance over critical systems.

Security awareness and education

Information Security is a shared responsibility across Contact.

Contact supports security awareness and education so our people understand information security expectations, know how to report concerns and can make secure decisions in their roles.

Awareness activity includes induction content, mandatory learning, targeted education, guidance, communications and exercises designed to reinforce secure behaviours and improve organisational resilience.

Third-party and supplier security

Contact works with suppliers and service providers who support technology, information and operational services.

Security considerations are included in supplier engagement and risk management activities, particularly where third parties can access, process or manage Contact information, systems or services.

Our programme includes ongoing improvement of third-party security posture management to help reduce the risk of information loss, operational disruption or compromise through supplier environments.

Assurance and independent review

Contact uses assurance activity to assess cybersecurity maturity, control effectiveness and opportunities for improvement.

This includes internal review, external assessment, maturity assessment, security testing and targeted assurance activities across technology and operational environments.

Findings are used to inform risk treatment, investment decisions, remediation roadmaps, governance reporting and continuous improvement of Contact's cybersecurity capability.

Continuous improvement

The Information Security Management Programme is continually improved as the threat environment, technology landscape and business needs evolve.

Improvement priorities are informed by risk assessment, assurance findings, technology change, maturity assessment, incident learnings and strategic priorities under Contact31+ and the Technology strategy.

This approach supports Contact's ability to strengthen resilience, protect information, manage material cyber risk and securely enable business transformation.