






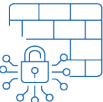











Practice Areas

| Icon | Practice area | Types of controls |
|---|---|--|
|  | Information Security Program Governance And Resourcing | - Information Security Program Policies And Standards Roles And Responsibilities, Risk Based Approach, Communication Of Security Program, Information Security Program Managing Non-Compliance, Continual Improvement. |
|  | Corporate Governance | - Standards And Certifications, Risk And Compliance, Audit, Reporting, Cyber Insurance. |
|  | Asset Management | - Inventory And Registration Of Assets, Maintenance, Return Of Assets, Secure Destruction. |
|  | Information Classification And Handling | - Information Classification, Information Handling, Data Retention And Destruction, Data Requests From Clients. |
|  | Identity And Access Management | - Account Provisioning, Access Control, Authentication Methods, Identity Management, Passwords, Account Reviews. |
|  | Application Security | - Application Security Controls, Secure Development. |
|  | Cryptography And Key Management | - Encryption In Transit, Encryption At Rest, Key Management. |
|  | Network Security And Content Filtering | - Network Design And Documentation, Network Security Features (Firewalls, Traffic Rules), Network Communications (Remote And Wireless Access), Content Filtering (Emails, DLP, Website And Application Whitelisting), Peripheral Devices (Mobile Devices And Removable Devices). |
|  | Business Continuity Disaster Recovery And Back Ups | - Business Continuity Plan, Backups, Disaster Recovery Plan, Capacity And Redundancy, Service Levels (RTO, RPO). |
|  | Logging And Monitoring | - Types Of Logs Collected, Log Management, Central Time Source, Monitoring And Alerting. |
|  | Incident Management | - Incident Response Plan, Incident Response Testing, Incident Event Management, Incident History. |
|  | Threat And Vulnerability Management | - Anti-Malware And Anti-Virus, Patch Management, Threat Intelligence, Vulnerability Scanning. |
|  | Human Resource Security | - Background Screening, Onboarding And Offboarding Of Employees, Termination Or Change Of Role, Company Training, Security Education And Awareness, Legal Agreements With Employees, Disciplinary Process. |
|  | Change Management | - Change Control Process, Restrict Unauthorised Changes, Security In Change. |
|  | Information Security Testing | - Testing Methods And Processes, Testing Resources, Managing Outcomes Of Testing. |
|  | Physical And Environmental Security | - Physical Access Control, Monitoring And Surveillance, Physical Asset Management, Perimeter And Restricted Areas, ICT Equipment, Environmental Controls, Cable Management, Physical Security Testing |
|  | Supply Chain Management | - Third Party Support, Third Party Access, Third Party Governance, Third Party Legal Agreements, Third Party Risk Assessments |

Disclaimer:

This Content is not comprehensive and is for general information purposes only. It does not take into account your specific needs, objectives or circumstances, and it is not advice. While we use reasonable attempts to ensure the accuracy and completeness of the Content, we make no representation or warranty in relation to it, to the maximum extent permitted by law. For further information about the use of InfoSecAssure tools and templates please refer to the InfoSecAssure Website Terms of Use.