ISO 27001:2013

Information, Security, Cybersecurity, and Privacy Protection

COMPASS
-ASSURANCE SERVICES-

SELF ASSESSMENT CHECKLIST

See how it works

CONTEXT

THE ORGANISATION

☐ Have we determined internal and external issues that will impact on our information security system?

INTERESTED PARTIES

☐ Have we determined what internal and external interested parties are relevant to the information security system and what are their requirements?

SCOPE

☐ Have we determined the boundaries of the information security system and documented the scope?

LEADERSHIP

LEADERSHIP & COMMITMENT

☐ Can we demonstrate top management is providing leadership and commitment to the information security system?

INFORMATION SECURITY SYSTEM

☐ Have we a documented information security policy that is communicated and available?

ROLES AND RESPONSIBILITIES

☐ Are roles and responsibilities for information security communicated and understood?

PLANNING

RISK & OPPORTUNITIES

- ☐ Have we determined the information security risk and opportunities related to our organization?

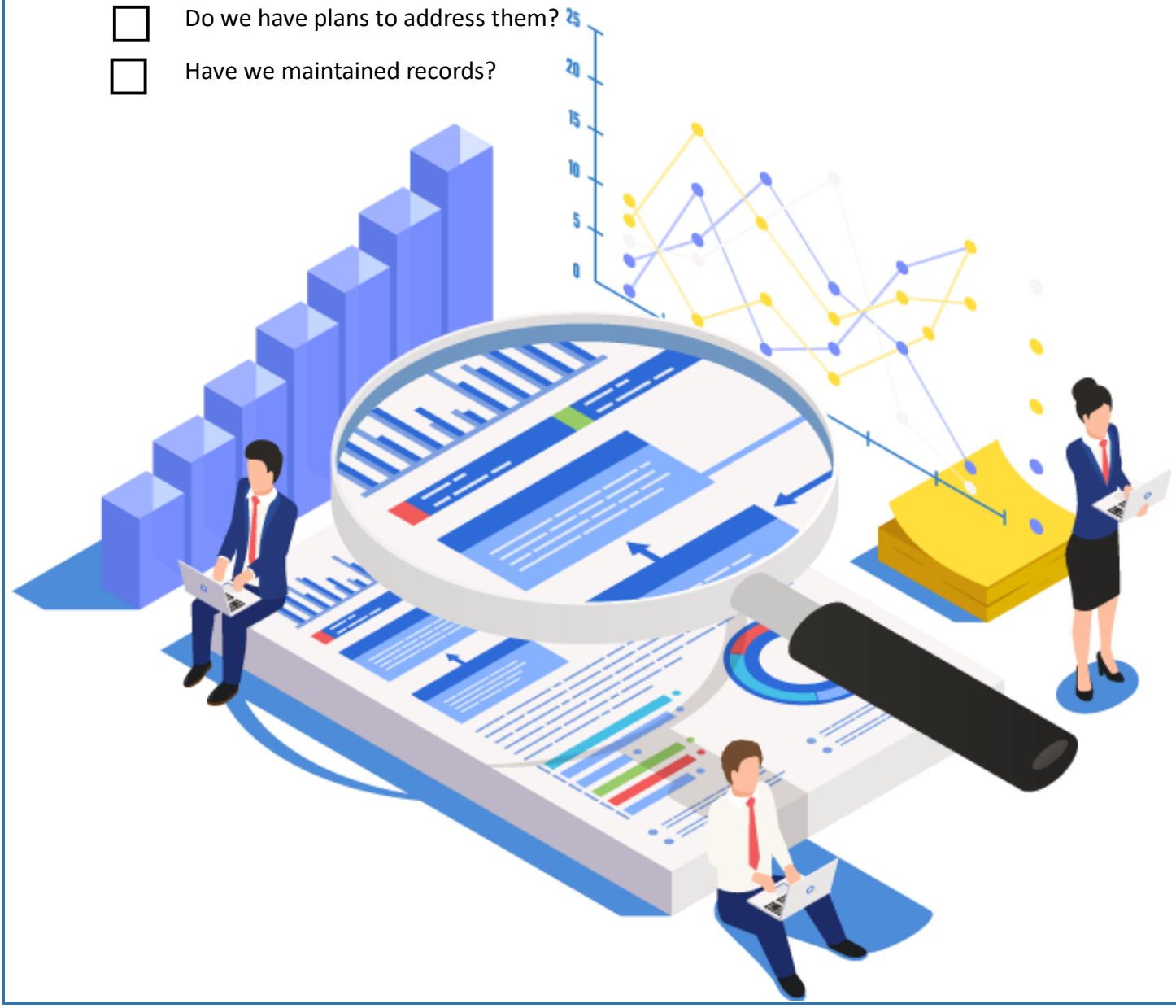
Have we implemented a documented information security risk assessment process?

STATEMENT OF APPLICABILITY

- ☐ Have we documented a risk treatment plan and statement of applicability with regard to controls?

INFORMATION SECURITY OBJECTIVES

- ☐ Have we established information security objectives?
- ☐ Do we monitor, measure, and communicate them?
- ☐ Do we have plans to address them?
- ☐ Have we maintained records?



SUPPORT

RESOURCES

- [ ] Have we determined and ensured necessary resources are in place for the information security system?

COMPETENCE

- [ ] Do we ensure the competence of personnel? Do we maintain records?

AWARENESS

- [ ] Have we ensured that personnel are aware of our policy, relevant objectives, and their responsibilities?

COMMUNICATION

- [ ] Have we determined processes for internal and external communication relevant to information security?

CONTROL OF DOCUMENTS

- [ ] Do we ensure documents and records are controlled?

OPERATIONS

OPERATIONAL PLANNING AND CONTROL

- [ ] Have we established and maintained procedures to meet the requirements of the information security system?

RISK ASSESSMENT AND TREATMENT

- [ ] Do we assess risk at planned intervals and when a significant change occurs?
- [ ] Have we implemented risk treatment plans?
- [ ] Do we maintain records?

PERFORMANCE EVALUATION

MONITORING & MEASUREMENT

- ☐ Do we monitor things such as processes, operational controls, access, usage, and change?
- ☐ Do we measure things such as KPI's and performance against targets?
- ☐ Do we analyze this information and maintain records?

INTERNAL AUDIT

- ☐ Do we plan and conduct internal audits to ensure the information security system conforms to requirements and is implemented effectively?
- ☐ Do we maintain records?

MANAGEMENT REVIEW

- ☐ Does our top management review our information security system at planned intervals?
- ☐ Do we maintain records?

IMPROVEMENT

NONCONFORMITY AND CORRECTIVE ACTION

☐ Do we have processes to manage preservation during production such as controls for packaging, handling, storage, and distribution?

CONTINUAL IMPROVEMENT

☐ Do we continually improve the information security system?

ANNEX A

A.5.1 Management Direction	A set of information security policies
A.6.1 Internal Organisation	Roles and responsibilities, segregation of duties, contact with relevant authorities, contact with special interest groups, information security implemented in project management
A6.2 Mobile Devices and Teleworking	A policy and measures for mobile devices A policy and measures for teleworking
A7.1 Prior to Employment	Prescreening of employees, information security terms and conditions of employment
A7.2 During Employment	Management's responsibility, awareness education, and training, disciplinary processes
A7.3 Termination and Change of Employment	Responsibilities post-employment
A8.1 Responsibility for Assets	Asset Inventory, ownership, acceptable use, return of assets
A8.2 Information Classification	Classification of information, labeling information, andhandling assets
A8.3 Media Handling	Managing removal of media, disposal of media, transferof media
A9.1 Access Control	Access Control Policy, Access to networks and network services
A9.2 User Access Management	Registration and de-registration, provisioning, privileges, authentication, access rights, removal of rights
A9.3 User Responsibility	Authentication responsibilities
A9.4 System and Application Access Control	Access, log-on procedures, password management, utility programs, access to source code
A10.1 Cryptography	Cryptography Policy, Key Management
A11.1 Secure Areas	Physical security perimeters, entry controls, securing offices and facilities, external and environmental threats, secure areas, delivery and loading docks
A11.2 Equipment	Equipment siting, support utilities, cabling, equipment maintenance, removal of assets, securing equipment offsite, unattended user equipment, clear desk, and clear screen

ANNEX A

A12.1 Operational Procedures and Responsibilities	Documented operational procedures, change management, capacity management, separation of development and testing
A12.2 Malware	Protection against malware
A12.3 Backup	Backups in place and tested regularly
A12.4 Logging and Monitoring	Event logging, storing log-in formation, administratorand operator logs, clock synchronization
A12.5 Operational Software	Protection of installed software
A12.6 Technical Vulnerability Management	Management of vulnerabilities, restrictions on software installation
A12.7 Information Security Audits	Audits and verification of operational systems
A13.1 Network Security Management	Network controls, network services security, segregation in networks
A13.2 Information Transfer	Transfer policies and procedures, external parties, Email, confidentiality and non-disclosure agreements
A14.1 Information Systems	Requirements, application services and public net-works, application service transactions
A14.2 Development and Support	Development Policy, System change procedures, Operating Platform changes, modification to software packages, secure system engineering, development environment, outsourced development, security testing, acceptance testing
A14.3 Test data	Protecting test data
A15.1 Supplier Relationships	Supplier access, supplier agreements, supply chain
A15.2 Supplier Services	Monitor and audit suppliers, changes to supplier services
A16.1 Incidents and Improvements	Incident responsibilities, reporting of incidents, re-porting weaknesses, assessment of events, incident response, learnings, collecting evidence
A17.1 Continuity	Continuity requirements, implementation of continuity processes, verifying and evaluating processes
A17.2 Redundancies	Ensuring information processing
A18.1 Compliance with Legal and Contractual Requirements	Documenting requirements, intellectual rights, pro-testing records, privacy, cryptographic regulations
A18.2 Security Reviews	Independent reviews, compliance with policies, technical compliance review

SO WHAT NOW?

Contact us for a quick quote to get a better idea of costs and timings. Visit our website

www.compasscertification.com