|  |  |  |  |
| --- | --- | --- | --- |
| **ΕΠΩΝΥΜΙΑ ΕΠΙΧΕΙΡΗΣΗΣ/ ΔΙΕΥΘΥΝΣΗ:** | **ΠΡΟΤΥΠΟ:** | **ΗΜΕΡΟΜΗΝΙΑ:** | **ΚΩΔΙΚΟΣ**  **ΕΡΓΟΥ:** |

|  |  |
| --- | --- |
| **ΣΥΜΜΕΤΕΧΟΝΤΕΣ EQA HELLAS (Ομάδα Επιθεώρησης):** | **ΣΥΜΜΕΤΕΧΟΝΤΕΣ ΠΕΛΑΤΗ:** |

|  |
| --- |
| **ΤΥΠΟΣ ΕΠΙΘΕΩΡΗΣΗΣ:** |
|  |

|  |  |
| --- | --- |
| **Σχόλια** (Ενδεικτικά:Περιγραφή μεταβολών από προηγούμενη επιθεώρηση (νομοθεσία, προϊόντα, διεργασίες, εγκαταστάσεις κλπ.) |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4.1 | Organization and context | Usually a diagram and an organizational chart as to where client’s team and operation resides and who are the Top Management stake holders. The documented process or procedure of holding a **strategy meeting** (or similar) where internal and external issues relevant to the ISMS are discussed.  Minutes of a **strategy meeting** (or similar) where management discussed various internal and external issues that were relevant to the ISMS – preferably within the past year. |  |  |
| 4.2 | Interested parties | Some sort of **list of stakeholders** in the ISMS, updated periodically (implying a procedure to formulate and maintain the list). This may include or reference lists of laws, regulations, contracts, agreements *etc*. that are relevant *i.e*. concern risks to and requirements for the security/protection/control of information. Internal corporate stakeholders in the ISMS should also be identified, including not just those who direct and oversee the ISMS but also those who depend on its correct operation (‘customers’ of the ISMS). |  |  |
| 4.3 | ISMS Scope | The **ISMS scope** clarifies the boundaries of the certified ISMS in relation to the context or business situation of the organization (*e.g*. certain business units, sites or departments), and its information risks and security requirements plus any imposed by third parties (*e.g*. laws and regulations plus contractual obligations and often, in a group structure, strategies and policies mandated). |  |  |
| 4.4 | ISMS | Intranet site, Document Management System or Governance Risk Compliance system. |  |  |
| 5.1 | Leadership | Evidence of management commitment to the ISMS may include their obvious interest and active involvement in the certification audit and other important ISMS activities (*e.g*. risk workshops), adequate **budgets**, **approval** of various formal documents (including budgets, expenditure and overspend/contingency), explicit reference to information risk and security in **strategies and plans** *etc*. |  |  |
| 5.2 | Information security policy | The **information security policy** (or policies) lays out and confirm senior management’s commitment to (a) the organization’s information security objectives and (b) continuous improvement of the ISMS and often much more. |  |  |
| 5.3 | Roles and responsibilities | The level or rank of the most senior information risk and security person (*e.g*. CISO or ISM) relative to other departments/functions, and the breadth of scope of the ISMS (*e.g*. buried within IT, limited to specific business units or organization-wide), are strong indications of how seriously management takes this. The governance arrangements are generally documented in **organization charts** showing reporting lines, **rôle/job descriptions**, **vacancy notices** *etc*. |  |  |
| 6.1.1 | Actions to address risks and οpportunities | This is a high-level requirement that the ISMS helps the organization manage its information risks and security controls systematically, on an ongoing basis. Evidence may include **strategy documents**, **vision statements**, minutes of **ISMS management meetings**, **corrective actions** Done, management and audit **recommendations** actioned, improving **metrics** *etc*. |  |  |
| 6.1.2 | Information security risk assessment Process documentation | It is up to you to determine precisely what is appropriate for your organization using clause 6.1.2 as a guideline plus [ISO/IEC 27005](http://www.iso27001security.com/html/27005.html) and ISO 31000. The auditors expect a structured and repeatable process *i.e.* a documented **risk assessment** **procedure** explaining how you identify, analyze (e.g. identify potential consequences and probabilities of occurrence), evaluate (*e.g.* use specified **criteria for risk acceptance**) and prioritize your information risks (e.g. using risk levels), with**periodic reviews/updates** to reflect gradual changes plus ***ad hoc* reviews/updates** in response to step-changes in their information risks. |  |  |
| 6.1.3 | Information security risk treatment  **Statement of Applicability** | The **Statement of Applicability** lays out the information risk and security controls that are relevant and applicable to organization’s ISMS, as determined by risk assessments or as required by laws, regulations or good practice. Cross-reference them against the controls recommended in ISO/IEC 27001 Annex A and ISO/IEDC 27002, plus any alternative/supplementary sources such as ISO 31000, ISO/IEC 20000, ISO 22301 and 22313. Clarify whether the controls recommended in ISO/IEC 27001 Annex A are in scope and appropriate to your organization, if not providing reasoned justifications (*e.g*. strategic management decisions, formally recorded) to convince the auditors that you haven’t simply neglected, ignored or arbitrarily excluded them. |  |  |
| 6.1.3 | Information security risk treatment  **Risk treatment process** | Again it is up to you to determine precisely what is appropriate for organization, using clause 6.1.3 plus guidance from [ISO/IEC 27005](http://www.iso27001security.com/html/27005.html) and ISO 31000. Risk treatment decisions (*e.g.* selecting treatments including applicable controls) and the actions arising (*e.g*. implementing the controls or sharing risks) may be an integral part of the risk assessment process, or a distinct activity or phase. Typical evidence includes a written **policy and/or** **procedure** for consistently deciding on and implementing appropriate information risk treatments. |  |
| 6.2 | Information security objectives and plans | The ISO requirement to “retain documented information on the information security objectives” is vague too, so once more you have some latitude. |  |  |
| 7.1 | Resources | ISMS resources are primarily people (**Full Time Equivalents**, **headcount** or **list** of permanent employees plus consultants, contractors, advisors, interns, temps *etc*.) and **budgets**. |  |  |
| 7.2 | Competence | **HR records** documenting the relevant experience, skills, qualifications, training courses *etc*. just for the core ISMS people within your information risk and security management function, or extend the net to include *all* the information risk, security, governance, privacy, business continuity and compliance-related people (and possibly otherssuch assecurity awareness and training professionals, departmental information security/privacy reps, business/security analysts, penetration testers *etc*., perhaps even consultants, contractors and advisors). |  |  |
| 7.3 | Awareness | Evidence for the security awareness activities includes any relevant procedures and standards, **awareness materials** (posters, presentations, briefings, web pages, leaflets, quizzes, competitions, training course notes, lists of rewards/prizes issued *etc*.) and **metrics** (*e.g.* records of attendance and feedback scores from awareness events, awareness survey and test results, and details of the ongoing investments in security awareness and training). |  |  |
| 7.4 | Communication | What the organization communicate regarding the ISMS, to whom, when and how, and gather relevant evidence about it – emails, notices, reports, metrics *etc*. Document the internal communications processes as well as collect evidence that shows them in operation. |  |  |
| 7.5.1 | General documentation | **This very checklist**, once completed and supported by the referenced documentation and records, is a simple way to demonstrate to the auditors the nature, breadth, volume and quality of information concerning and generated by your ISMS. |  |  |
| 7.5.2 | Creating and updating docs | The revision history, and any authorizations or mandates. |  |  |
| 7.5.3 | Control of docs | Document management systems and webservers can generate reports of **access rights**, document **status** *etc*. for policies, procedures and guidelines *etc*. Emails, management reports, review and audit reports, metrics reports *etc*. generally state their own distribution on the cover, or may use **classification** rules or managed **distribution lists**. |  |  |
| 8.1 | Operational planning and control  **Procedures** | Keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. Generally speaking, this implies **management information** concerning the ISMS such as **budgets** and **headcounts** and **progress reports** containing relevant **metrics,** information risk and security **strategies, plans, policies, procedures** and **guidelines**, plus related **compliance activities** to check/measure, enforce and reinforce compliance, plus **records** generated by or information arising from the procedures/activities, and other stuff such as post incident reports, security test reports, security product evaluations, vulnerability assessments, business impact assessments, preventive or corrective actions, security architectures and designs. |  |  |
| 8.2 | Risk assessment results | Information should be generated routinely by the risk assessment process noted in section 6.1.2. Examples include **risk assessment reports, risk metrics, prioritized lists of risks, information risk inventories or catalogs** or information risk entries in corporate risk inventories/catalogs *etc*. |  |  |
| 8.3 | Risk treatment results | How are you going to prove that identified information risks are being ‘treated’ in accordance with the process and decisions made? The **Risk Treatment Plan** might usefully reference evidence/records confirming that risks have been and are being duly treated, such as **control test reports**, **penetration test reports**, **control implementation project plans** plus milestones and closure documents, purchasing and financial records for **capital expenditure**, **metrics** showing a reduction in the frequency and/or severity of the corresponding incidents *etc*., **management review and audit reports**, emails from management congratulating the ISMS team and awarding large bonuses *etc*. |  |  |
| 9.1 | Metrics | The ISMS generates various metrics that are used to monitor and drive information risks, controls and the ISMS itself in the intended direction. Evidence here includes **security metrics** in reports, systems, dashboards, presentations *etc*., plus proof that the metrics are being duly noted and acted upon *e.g*. memos, emails or rough notes expressing concern about adverse trends or thanks for positive trends; comments scribbled on printed reports; action plans; minutes of meetings *etc*. |  |  |
| 9.2 | ISMS internal audits | **ISMS internal audit reports** are the obvious evidence here, documenting the main audit findings, conclusions and recommendations, often in the form of Nonconformity/Corrective Action Reports. Supporting evidence may include audit programs or plans or calendars, budgets and auditor man-day allocations, audit scopes, audit working paper files with detailed audit findings and evidence (such as completed checklists), audit recommendations, agreed action plans and closure notes *etc*. |  |  |
| 9.3 | ISMS management reviews | **ISMS management review reports,** obviously, perhaps also calendars/plans, budgets, scopes, working papers with evidence, recommendations, action plans, closure notes *etc*. The certification auditors *may* want to interview/chat to relevant Top Management and managers about the ISMS and/or issues raised in their reports. |  |  |
| 10.1 | Nonconformities and corrective actions | ‘Nonconformities’ are (partially or wholly) unsatisfied requirements, including those within [ISO/IEC 27001](http://www.iso27001security.com/html/27001.html), plus strategies, policies, procedures, guidelines, laws, regulations and contracts. They may be documented in the form of issues, events, incidents, audit and review findings, complaints, or simply as “nonconformities” |  |  |
| 10.2 | Continual improvement | Documentary evidence for continual improvement of the ISMS includes the reports of **reviews, audits, incidents, corrective actions, ISMS strategy/planning and management meetings** plus assorted **metrics** demonstrating positive trends. |  |  |

**Γ. Έλεγχοι σύμφωνα με το Παράρτημα Α Αναφορά στους στόχους ελέγχου και έλεγχοι.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.5** | **Information Security Policies** | | | |
| **A.5.1** | **Management direction for information security** | | | |
| A.5.1.1 | Policies for information security | 1. Do Security policies exist? 2. Are all policies approved by management? 3. Are policies properly communicated to employees? |  |  |
| A.5.1.2 | Review of the policies for information security | 1. Are security policies subject to review? 2. Are the reviews conducted at regular intervals? 3. Are reviews conducted when circumstances change? |  |
| **A.6** | **Organisation of information security** | | | |
| **A.6.1** | **Internal Organisation** | | | |
| A.6.1.1 | Information security roles and responsibilities | Are responsibilities for the protection of individual assets, and for carrying out specific security processes, clearly identified and defined and communicated to the relevant  parties? |  |  |
| A.6.1.2 | Segregation of duties | Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services? |  |
| A.6.1.3 | Contact with authorities | 1. Is there a procedure documenting when, and by whom, contact with relevant authorities (law enforcement etc.) will be made? 2. Is there a process which details how and when contact is required? 3. Is there a process for routine contact and   intelligence sharing? |  |
| A.6.1.4 | Contact with special interest groups | Do relevant individuals within the organisation maintain active membership in relevant special interest groups? |  |
| A.6.1.5 | Information security in project  management | Do all projects go through some form of  information security assessment? |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A.6.2.1 | Mobile device policy | 1. Is there a policy for mobile devices? 2. Does this have management approval? |  |  |
| A.6.2.2 | Teleworking | 1. Is there a policy for teleworking? 2. Does this have management approval? 3. Is there a set process for remote workers to get access? 4. Are teleworkers given the advice and   equipment to protect their assets? |  |
| **A.7** | **Human Resource Security** | | | |
| **A.7.1** | ***Prior to employment*** | | | |
| A.7.1.1 | Screening | 1. Are background verification checks carried out on all new candidates for employment? 2. Are these checks approved by appropriate management authority? 3. Are the checks compliant with relevant laws, regulations and ethics? 4. Are the level of checks required supported by business risk assessments? |  |  |
| A.7.1.2 | Terms and conditions of employment | 1. Are all employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements? 2. Do employment / service contracts specifically cover the need to protect business information? |  |
| **A.7.2** | ***During employment*** | | | |
| A.7.2.1 | Management responsibilities | 1. Are managers (of all levels) engaged in driving security within the business? 2. Does management behaviour and policy drive, and encourage, all employees, contractors and 3rd party users to apply security in accordance with established policies and procedures? |  |  |
| A.7.2.2 | Information security awareness, education and training | Do all employees, contractors and 3rd party users undergo regular security awareness training appropriate to their role and function within the organization? |  |
| A.7.2.3 | Disciplinary process | 1. Is there a formal disciplinary process which allows the organization to take action against employees who have committed an information security breach? 2. Is this communicated to all employees? |  |
| **A.7.3** | **Termination and change of employment** | | | |
| A.7.3.1 | Termination or change of employment responsibilities | 1. Is there a documented process for terminating or changing employment duties? 2. Are any information security duties which survive employment communicated to the employee or contractor? 3. Is the organisation able to enforce compliance with any duties that survive employment? |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.8** | **Asset management** | | | |
| **A.8.1** | **Responsibility for assets** | | | |
| A.8.1.1 | Inventory of assets | 1. Is there an inventory of all assets associated with information and information processing facilities? 2. Is the inventory accurate and kept up to   date? | . |  |
| A.8.1.2 | Ownership of assets | All information assets must have a clearly  defined owner who is aware of their responsibilities. |  |
| A.8.1.3 | Acceptable use of assets | 1. Is there an acceptable use policy for each class / type of information asset? 2. Are users made aware of this policy prior to   use? |  |
| A.8.1.4 | Return of assets | Is there a process in place to ensure all employees and external users return the organisation's assets on termination of their employment, contract or agreement? |  |
| **A.8.2** | **Information classification** | | | |
| A.8.2.1 | Classification of information | 1. Is there a policy governing information classification? 2. Is there a process by which all information can be appropriately classified? |  |  |
| A.8.2.2 | Labelling of information | Is there a process or procedure for ensuring information classification is appropriately  marked on each asset? |  |
| A.8.2.3 | Handling of assets | 1. Is there a procedure for handling each information classification? 2. Are users of information assets made aware   of this procedure? |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.8.3** | **Media handling** | | | |
| A.8.3.1 | Management of removable media | 1. Is there a policy governing removable media? 2. Is there a process covering how removable media is managed? 3. Are the policy and process(es) communicated to all employees using   removable media? |  |  |
| A.8.3.2 | Disposal of media | Is there a formal procedure governing how  removable media is disposed? |  |
| A.8.3.3 | Physical media transfer | 1. Is there a documented policy and process detailing how physical media should be transported? 2. Is media in transport protected against unauthorised access, misuse or corruption? |  |
| **A.9** | **Access control** | | | |
| **A.9.1** | **Business requirements for access control** | | | |
| A.9.1.1 | Access control policy | 1. Is there a documented access control policy? 2. Is the policy based on business requirements? 3. Is the policy communicated appropriately? |  |  |
| A.9.1.2 | Access to networks and network services | Are controls in place to ensure users only have access to the network resources they have been specially authorized to use and are required for their duties? |  |
| **A.9.2** | **User access management** | | | |
| A.9.2.1 | User registration and de-registration | Is there a formal user access registration  process in place? |  |  |
| A.9.2.2 | User access provisioning | Is there a formal user access provisioning process in place to assign access rights for all  user types and services? |  |
| A.9.2.3 | Management of privileged access rights | Are privileged access accounts separately  managed and controlled? |  |
| A.9.2.4 | Management of secret authentication information of users | Is there a formal management process in place  to control allocation of secret authentication information? |  |
| A.9.2.5 | Review of user access rights | 1. Is there a process for asset owners to review access rights to their assets on a regular basis? 2. Is this review process verified? |  |
| A.9.2.6 | Removal or adjustment of access rights | Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role? |  |
| **A.9.3** | **User responsibilities** | | | |
| A.9.3.1 | Use of secret authentication information | 1. Is there a policy document covering the organisations practices in how secret authentication information must be handled? 2. Is this communicated to all users? |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.9.4** | **System and application access control** | | | |
| A.9.4.1 | Information access restriction | Is access to information and application  system functions restricted in line with the access control policy? |  |  |
| A.9.4.2 | Secure log-on procedures | Where the access control policy requires it, is access controlled by a secure log-on  procedure? |  |
| A.9.4.3 | Password management system | 1. Are password systems interactive? 2. Are complex passwords required? |  |
| A.9.4.4 | Use of privileged utility programs | Are privilege utility programs restricted and  monitored? |  |
| A.9.4.5 | Access control to program source code | Is access to the source code of the Access  Control System protected? |  |
| **A.10** | **Cryptography** | | | |
| **A.10.1** | **Cryptographic controls** | | | |
| A.10.1.1 | Policy on the use of cryptographic controls | Is there a policy on the use of cryptographic  controls? |  |  |
| A.10.1.2 | Key management | Is there a policy governing the whole lifecycle  of cryptographic keys? |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.11** | **Physical and environmental security** | | | |
| **A.11.1** | **Secure areas** | | | |
| A.11.1.1 | Physical security perimeter | 1. Is there a designated security perimeter? 2. Are sensitive or critical information areas segregated and appropriately controlled? |  |  |
| A.11.1.2 | Physical entry controls | Do secure areas have suitable entry control systems to ensure only authorized personnel  have access? |  |
| A.11.1.3 | Securing offices, rooms and facilities | 1. Have offices, rooms and facilities been designed and configured with security in mind? 2. Do processes for maintaining the security (e.g. Locking up, clear desks etc.) exist? |  |
| A.11.1.4 | Protecting against external and environmental threats | Have physical protection measures to prevent natural disasters, malicious attack or accidents  been designed in? |  |
| A.11.1.5 | Working in secure areas | 1. Do secure areas exist? 2. Where they do exist, do secure areas have suitable policies and processes? 3. Are the policies and processes enforced and   monitored? |  |
| A.11.1.6 | Delivery and loading areas | 1. Are there separate delivery / loading areas? 2. Is access to these areas controls? 3. Is access from loading areas isolated from information processing facilities? |  |
| **A.11.2** | **Equipment** | | | |
| A.11.2.1 | Equipment siting and protection | 1. Are environmental hazards identified and considered when equipment locations are selected? 2. Are the risks from unauthorised access / passers-by considered when siting equipment? |  |  |
| A.11.2.2 | Supporting utilities | 1. Is there a UPS system or back up generator? 2. Have these been tested within an appropriate timescale? |  |
| A.11.2.3 | Cabling security | 1. Have risk assessments been conducted over the location of power and telecommunications cables? 2. Are they located to protect from   interference, interception or damage? |  |
| A.11.2.4 | Equipment maintenance | Is there a rigorous equipment maintenance  schedule? |  |
| A.11.2.5 | Removal of assets | 1. Is there a process controlling how assets are removed from site? 2. Is this process enforced? 3. Are spot checks carried out? |  |
| A.11.2.6 | Security of equipment and assets off- premises | 1. Is there a policy covering security of assets off-site? 2. Is this policy widely communicated? |  |
| A.11.2.7 | Secure disposal or reuse of equipment | 1. Is there a policy covering how information assets may be reused? 2. Where data is wiped, is this properly verified   before reuse/disposal? |  |
| A.11.2.8 | Unattended user equipment | 1. Does the organisation have a policy around how unattended equipment should be protected? 2. Are technical controls in place to secure equipment that has been inadvertently left   unattended? |  |
| A.11.2.9 | Clear desk and clear screen policy | 1. Is there a clear desk / clear screen policy? 2. Is this well enforced? |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.12** | **Operations security** | | | |
| **A.12.1** | **Operational procedures and responsibilities** | | | |
| A.12.1.1 | Documented operating procedures | 1. Are operating procedures well documented? 2. Are the procedures made available to all   users who need them? |  |  |
| A.12.1.2 | Change management | Is there a controlled change management  process in place? |  |
| A.12.1.3 | Capacity management | Is there a capacity management process in  place? |  |
| A.12.1.4 | Separation of development, testing and operational environments | Does the organisation enforce segregation of development, test and operational  environments? |  |
| **A.12.2** | **Protection from malware** | | | |
| A.12.2.1 | Controls against malware | 1. Are processes to detect malware in place? 2. Are processes to prevent malware spreading in place? 3. Does the organisation have a process and capacity to recover from a malware infection. |  |  |
| **A.12.3** | **Backup** | | | |
| A.12.3.1 | Information backup | 1. Is there an agreed backup policy? 2. Does the organisation's backup policy comply with relevant legal frameworks? 3. Are backups made in accordance with the policy? 4. Are backups tested? |  |  |
| **A.12.4** | **Logging and monitoring** | | | |
| A.12.4.1 | Event logging | Are appropriate event logs maintained and  regularly reviewed? |  |  |
| A.12.4.2 | Protection of log information | Are logging facilities protected against  tampering and unauthorised access? |  |
| A.12.4.3 | Administrator and operator logs | Are sysadmin / sysop logs maintained,  protected and regularly reviewed? |  |
| A.12.4.4 | Clock synchronisation | Are all clocks within the organisation |  |
| **A.12.5** | **Control of operational software** | | | |
| A.12.5.1 | Installation of software on operational systems | Is there a process in place to control the  installation of software onto operational systems? |  |  |
| **A.12.6** | **Technical vulnerability management** | | | |
| A.12.6.1 | Management of technical vulnerabilities | 1. Does the organisation have access to updated and timely information on technical vulnerabilities? 2. Is there a process to risk assess and react to any new vulnerabilities as they are   discovered? |  |  |
| A.12.6.2 | Restrictions on soft-ware installation | Are there processes in place to restrict how  users install software? |  |
| **A.12.7** | **Information systems audit considerations** | | | |
| A.12.7.1 | Information systems audit controls | 1. Are IS Systems subject to audit? 2. Does the audit process ensure business disruption is minimised? |  |  |
| **A.13** | **Communications security** | | | |
| **A.13.1** | **Network security management** | | | |
| A.13.1.1 | Network controls | Is there a network management process in  place? |  |  |
| A.13.1.2 | Security of network services | 1. Does the organisation implement a risk management approach which identifies all network services and service agreements? 2. Is security mandated in agreements and contracts with service providers (in house and outsourced). 3. Are security related SLAs mandated? |  |
| A.13.1.3 | Segregation in networks | Does the network topology enforce segregation of networks for different tasks? |  |
| **A.13.2** | **Information transfer** | | | |
| A.13.2.1 | Information transfer policies and procedures | 1. Do organizational policies govern how information is transferred? 2. Are procedures for how data should be transferred made available to all employees? 3. Are relevant technical controls in place to prevent non-authorized forms of data transfer? |  |  |
| A.13.2.2 | Agreements on information transfer | Do contracts with external parties and agreements within the organisation detail the requirements for securing business  information in transfer? |  |
| A.13.2.3 | Electronic messaging | Do security policies cover the use of information transfer while using electronic  messaging systems? |  |
| A.13.2.4 | Confidentiality or nondisclosure agreements | 1. Do employees, contractors and agents sign confidentiality or non disclosure agreements? 2. Are these agreements subject to regular review? 3. Are records of the agreements maintained? |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.14** | **System acquisition, development and maintenance** | | | |
| **A.14.1** | **Security requirements of information systems** | | | |
| A.14.1.1 | Information security requirements analysis and specification | 1. Are information security requirements specified when new systems are introduced? 2. When systems are being enhanced or upgraded, are security requirements specified and addressed? | . |  |
| A.14.1.2 | Securing application services on public networks | Do applications which send information over public networks appropriately protect the information against fraudulent activity, contract dispute, unauthorised discloser and unauthorised modification? |  |
| A.14.1.3 | Protecting application services transactions | Are controls in place to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay  attacks? |  |
| **A.14.2** | **Security in development and support processes** | | | |
| A.14.2.1 | Secure development policy | 1. Does the organisation develop software or systems? 2. If so, are there policies mandating the implementation and assessment of security   controls? |  |  |
| A.14.2.2 | System change control procedures | Is there a formal change control process? |  |
| A.14.2.3 | Technical review of applications after operating platform changes | Is there a process to ensure a technical review is carried out when operating platforms are  changed? |  |
| A.14.2.4 | Restrictions on changes to software packages | Is there a policy in place which mandates when and how software packages can be changed or  modified? |  |
| A.14.2.5 | Secure system engineering principles | Does the organisation have documented principles on how systems must be engineered  to ensure security? |  |
| A.14.2.6 | Secure development environment | 1. Has a secure development environment been established? 2. Do all projects utilise the secure development environment appropriately during the system development lifecycle? |  |
| A.14.2.7 | Outsourced development | 1. Where development has been outsourced is this supervised? 2. Is externally developed code subject to a   security review before deployment? |  |
| A.14.2.8 | System security testing | Where systems or applications are developed, are they security tested as part of the  development process? |  |
| A.14.2.9 | System acceptance testing | Is there an established process to accept new systems / applications, or upgrades, into  production use? |  |
| **A.14.3** | **Test data** | | | |
| A.14.3.1 | Protection of test data | 1. Is there a process for selecting test data? 2. Is test data suitably protected? |  |  |
| A.15 | Supplier relationships | | | |
| **A.15.1** | **Information security in supplier relationships** | | | |
| A.15.1.1 | Information security policy for supplier relationships | 1. Is information security included in contracts established with suppliers and service providers? 2. Is there an organisation-wide risk management approach to supplier   relationships? |  |  |
| A.15.1.2 | Addressing security within supplier agreements | 1. Are suppliers provided with documented security requirements? 2. Is supplier access to information assets & infrastructure controlled and monitored? |  |
| A.15.1.3 | Information and communication technology supply chain | Do supplier agreements include requirements to address information security within the service & product supply chain? |  |
| **A.15.2** | **Supplier service delivery management** | | | |
| A.15.2.1 | Monitoring and review of supplier services | Are suppliers subject to regular review and  audit? |  |  |
| A.15.2.2 | Managing changes to supplier services | Are changes to the provision of services subject to a management process which  includes security & risk assessment? |  |
| **A.16** | **Information security incident management** | | | |
| **A.16.1** | **Management of information security incidents and improvements** | | | |
| A.16.1.1 | Responsibilities and procedures | Are management responsibilities clearly identified and documented in the incident  management processes? |  |  |
| A.16.1.2 | Reporting information security events | 1. Is there a process for timely reporting of information security events? 2. Is there a process for reviewing and acting on reported information security events? |  |
| A.16.1.3 | Reporting information security weaknesses | 1. Is there a process for reporting of identified information security weaknesses? 2. Is this process widely communicated? 3. Is there a process for reviewing and addressing reports in a timely manner? |  |
| A.16.1.4 | Assessment of and decision on information security events | Is there a process to ensure information security events are properly assessed and  classified? |  |
| A.16.1.5 | Response to information security incidents | Is there an incident response process which reflects the classification and severity of information security incidents? |  |
| A.16.1.6 | Learning from information security incidents | Is there a process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events? |  |
| A.16.1.7 | Collection of evidence | 1. Is there a forensic readiness policy? 2. In the event of an information security incident is relevant data collected in a manner which allows it to be used as evidence? |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.17** | **Information security aspects of business continuity management** | | | |
| **A.17.1** | **Information security continuity** | | | |
| A.17.1.1 | Planning information security continuity | Is information security included in the  organisation's continuity plans? |  |  |
| A.17.1.2 | Implementing information security continuity | Does the organisation's information security function have documented, implemented and maintained processes to maintain continuity of service during an adverse situation? |  |
| A.17.1.3 | Verify, review and evaluate information  security continuity | Are continuity plans validated and verified at  regular intervals? |  |
| **A.17.2** | **Redundancies** | | | |
| A.17.2.1 | Availability of information processing facilities | Do information processing facilities have sufficient redundancy to meet the  organisations availability requirements? |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **A.18** | **Compliance** | | | |
| **A.18.1** | **Compliance with legal and contractual requirements** | | | |
| A.18.1.1 | Identification of applicable legislation and contractual requirements | 1. Has the organisation identified and documented all relevant legislative, regulatory or contractual requirements related to security? 2. Is compliance documented? |  |  |
| A.18.1.2 | Intellectual property rights | 1. Does the organisation keep a record of all intellectual property rights and use of proprietary software products? 2. Does the organisation monitor for the use of   unlicensed software? |  |
| A.18.1.3 | Protection of records | Are records protected from loss, destruction, falsification and unauthorised access or release in accordance with legislative, regulatory, contractual and business  requirements? |  |
| A.18.1.4 | Privacy and protection of personally identifiable information | 1. Is personal data identified and appropriately classified? 2. Is personal data protected in accordance   with relevant legislation? |  |
| A.18.1.5 | Regulation of cryptographic controls | Are cryptographic controls protected in  accordance with all relevant agreements, legislation and regulations? |  |
| **A.18.2** | **Information security reviews** | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A.18.2.1 | Independent review of information security | 1. Is the organisations approach to managing information security subject to regular independent review? 2. Is the implementation of security controls subject to regular independent review? |  |  |
| A.18.2.2 | Compliance with security policies and standards | 1. Does the organisation instruct managers to regularly review compliance with policy and procedures within their area of responsibility? 2. Are records of these reviews maintained? |  |
| A.18.2.3 | Technical compliance review | Does the organisation regularly conduct technical compliance reviews of its  information systems? |  |