**[](https://www.smartsheet.com/try-it?trp=11680&utm_source=integrated-content&utm_campaign=/cyber-security-assessment-templates&utm_medium=Sample+Cybersecurity+Risk+Assessment+Checklist+doc+11680&lpa=Sample+Cybersecurity+Risk+Assessment+Checklist+doc+11680)CYBER SECURITY RISK ASSESSMENT   
CHECKLIST TEMPLATE EXAMPLE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ISO 27001 CONTROL** | **IMPLEMENTATION PHASES** | **TASKS** | **IN COMPLIANCE?** | **NOTES** |
| **5** | ***Information security policies*** | | | |
| **5.1** | **Management direction for information security** | | | |
|  |  | Security policies exist? | **x** |  |
| 5.1.1  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | Policies for information security | All policies approved by management? | **x** |  |
|  |  | Evidence of compliance? |  |  |
| **6** | ***Organization of information security*** | | | |
| **6.1** | **Information security roles and responsibilities** | | | |
| 6.1.1 | Security roles and responsibilities | Roles and responsibilities defined? | **x** |  |
| 6.1.2 | Segregation of duties | Segregation of duties defined? | **x** |  |
| 6.1.3 | Contact with authorities | Verification body / authority contacted for compliance verification? |  |  |
| 6.1.4 | Contact with special interest groups | Establish contact with special interest groups regarding compliance? | **x** |  |
| 6.1.5 | Information security in project management | Evidence of information security in project management? |  |  |
| **6.2** | **Mobile devices and teleworking** | | | |
| 6.2.1  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | Mobile device policy | Defined policy for mobile devices? |  |  |
| 6.2.2 | Teleworking | Defined policy for working remotely? |  |  |
|  |  |  |  |  |
| **7** | ***Human resources security*** | | | |
| **7.1** | **Prior to employment** | | | |
| 7.1.1 | Screening | Defined policy for screening employees prior to employment? |  |  |
| 7.1.2 | Terms and conditions of employment | Defined policy for HR terms and conditions of employment? |  |  |
| **7.2** | **During employment** | | | |
| 7.2.1 | Management responsibilities | Defined policy for management responsibilities? |  |  |
| 7.2.2 | Information security awareness, education, and training | Defined policy for information security awareness, education,  and training? |  |  |
| 7.2.3 | Disciplinary process | Defined policy for  disciplinary process regarding information security? |  |  |
| **7.3**  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | **Termination and change of employment** | | | |
| 7.3.1 | Termination or change-of-employment responsibilities | Defined policy for HR termination or change-of-employment policy regarding information security? |  |  |
| **8** | ***Asset management*** | | | |
| **8.1** | **Responsibilities for assets** | | | |
| 8.1.1 | Inventory of assets | Complete inventory list of assets? |  |  |
| 8.1.2 | Ownership of assets | Complete ownership list of assets |  |  |
| 8.1.3 | Acceptable use of assets | Defined acceptable use of assets policy |  |  |
| 8.1.4 | Return of assets | Defined return of assets policy? |  |  |
| **8.2** | **Information classification** | | | |
| 8.2.1 | Classification of information | Defined policy for classification  of information? |  |  |
| 8.2.2 | Labeling of information | Defined policy for labeling of information? |  |  |
| 8.2.3 | Handling of assets | Defined policy for handling  of assets? |  |  |
| **8.3** | **Media handling** | | | |
| 8.3.1 | Management of removable media | Defined policy for management  of removable media? |  |  |
| 8.3.2  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | Disposal of media | Defined policy for disposal of media? |  |  |
| 8.3.3. | Physical media transfer | Defined policy for physical  media transfer? |  |  |
| **9** | ***Access control*** | | | |
| **9.1** | **Responsibilities for assets** | | | |
| 9.1.1 | Access control policy | Defined policy for access  control? |  |  |
| 9.1.2 | Access to networks and  network services | Defined policy for access to networks and network services? |  |  |
| **9.2** | **Responsibilities for assets** | | | |
| 9.2.1 | User asset registration and de-registration | Defined policy for user asset registration and de-registration? |  |  |
| 9.2.2 | User access provisioning | Defined policy for user access provisioning? |  |  |
| 9.2.3 | Management of privileged  access rights | Defined policy for management  of privileged access rights? |  |  |
| 9.2.4 | Management of secret authentication information of users | Defined policy for management  of secret authentication  information of users? |  |  |
| 9.2.5 | Review of user access rights | Defined policy for review of user access rights? |  |  |
| 9.2.6 | Removal or adjustment  of access rights | Defined policy for removal or adjustment of access rights? |  |  |
| **9.3** | **User responsibilities** | | | |
| 9.3.1 | Use of secret authentication information | Defined policy for use of secret authentication information? |  |  |
| **9.4** | **System and application access control** | | | |
| 9.4.1 | Information access restrictions | Defined policy for information access restrictions? |  |  |
| 9.4.2 | Secure log-in procedures | Defined policy for secure log-in procedures? |  |  |
| 9.4.3 | Password management systems | Defined policy for password management systems? |  |  |
| 9.4.4  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | Use of privileged utility programs | Defined policy for use of privileged utility programs? |  |  |
| 9.4.5 | Access control to program source code | Defined policy for access control  to program source code? |  |  |
| **10** | ***Cryptography*** | | | |
| **10.1** | **Cryptographic controls** | | | |
| 10.1.1  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | Policy for the use of  cryptographic controls | Defined policy for use of cryptographic controls? |  |  |
| 10.1.2 | Key management | Defined policy for key management? |  |  |
| **11** | ***Physical and environmental security*** | | | |
| **11.1** | **Secure areas** | | | |
| 11.1.1 | Physical security perimeter | Defined policy for physical security perimeter? |  |  |
| 11.1.2 | Physical entry controls | Defined policy for physical entry controls? |  |  |
| 11.1.3 | Securing offices, rooms, and facilities | Defined policy for securing offices, rooms, and facilities? |  |  |
| 11.1.4 | Protection against external and environmental threats | Defined policy for protection against external and environmental threats? |  |  |
| 11.1.5 | Working in secure areas | Defined policy for working in secure areas? |  |  |
| 11.1.6 | Delivery and loading areas | Defined policy for delivery and loading areas? |  |  |
| **11.2** | **Equipment** | | | |
| 11.2.1 | Equipment siting and protection | Defined policy for equipment siting and protection? |  |  |
| 11.2.2 | Supporting utilities | Defined policy for supporting utilities? |  |  |
| 11.2.3 | Cabling security | Defined policy for cabling security? |  |  |
| 11.2.4 | Equipment maintenance | Defined policy for equipment maintenance? |  |  |
| 11.2.5 | Removal of assets | Defined policy for removal of assets? |  |  |
| 11.2.6 | Security of equipment and assets off-premises | Defined policy for security of equipment and assets off-premises? |  |  |
| 11.2.7 | Secure disposal or re-use of equipment | Secure disposal or re-use of equipment? |  |  |
| 11.2.8  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | Unattended user equipment | Defined policy for unattended user equipment? |  |  |
| 11.2.9 | Clear desk and clear screen policy | Defined policy for clear desk and clear screen policy? |  |  |
| **12** | ***Operations security*** | | | |
| **12.1** | **Operational procedures and responsibilities** | | | |
| 12.1.1 | Documented operating procedures | Defined policy for documented operating procedures? |  |  |
| 12.1.2 | Change management | Defined policy for change management? |  |  |
| 12.1.3 | Capacity management | Defined policy for capacity management? |  |  |
| 12.1.4 | Separation of development, testing, and operational environments | Defined policy for separation of development, testing, and operational environments? |  |  |
| **12.2** | **Protection from malware** | | | |
| 12.2.1 | Controls against malware | Defined policy for controls against malware? |  |  |
| **12.3** | **System backup** | | | |
| 12.3.1 | Backup | Defined policy for backing up systems? |  |  |
| 12.3.2 | Information Backup | Defined policy for information backup? |  |  |
| **12.4** | **Logging and monitoring** | | | |
| 12.4.1 | Event logging | Defined policy for event logging? |  |  |
| 12.4.2 | Protection of log information | Defined policy for protection of  log information? |  |  |
| 12.4.3 | Administrator and operator log | Defined policy for administrator and operator log? |  |  |
| 12.4.4 | Clock synchronization | Defined policy for clock synchronization? |  |  |
| **12.5** | **Control of operational software** | | | |
| 12.5.1 | Installation of software on operational systems | Defined policy for installation of software on operational systems? |  |  |
| **12.6** | **Technical vulnerability management** | | | |
| 12.6.1 | Management of technical vulnerabilities | Defined policy for management of technical vulnerabilities? |  |  |
| 12.6.2 | Restriction on software installation | Defined policy for restriction on software installation? |  |  |
| **12.7**  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | **Information systems audit considerations** | | | |
| 12.7.1 | Information system audit control | Defined policy for information system audit control? |  |  |
| **13** | ***Communication security*** | | | |
| **13.1** | **Network security management** | | | |
| 13.1.1 | Network controls | Defined policy for network controls? |  |  |
| 13.1.2 | Security of network services | Defined policy for security of network services? |  |  |
| 13.1.3 | Segregation in networks | Defined policy for segregation in networks? |  |  |
| **13.2** | **Information transfer** | | | |
| 13.2.1 | Information transfer policies and procedures | Defined policy for information transfer policies and procedures? |  |  |
| 13.2.2 | Agreements on information transfer | Defined policy for agreements on information transfer? |  |  |
| 13.2.3 | Electronic messaging | Defined policy for electronic messaging? |  |  |
| 13.2.4  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | Confidentiality or non-disclosure agreements | Defined policy for confidentiality or non-disclosure agreements? |  |  |
| 13.2.5 | System acquisition, development, and maintenance | Defined policy for system acquisition, development, and maintenance? |  |  |
| **14** | ***System acquisition, development, and maintenance*** | | | |
| **14.1** | **Security requirements of information systems** | | | |
| 14.1.1 | Information security requirements analysis and specification | Defined policy for information security requirements analysis and specification? |  |  |
| 14.1.2 | Securing application services on public networks | Defined policy for securing application services on public networks? |  |  |
| 14.1.3 | Protecting application service transactions | Defined policy for protecting application service transactions? |  |  |
| **14.2**  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | **Security in development and support processes** | | | |
| 14.2.1 | In-house development | Defined policy for in-house development? |  |  |
| **15** | ***Supplier relationships*** | | | |
| 15.1.1 | Supplier relationships | Defined policy for supplier relationships? |  |  |
| **16** | ***Information security incident management*** | | | |
| 16.1.1 | Information security management | Defined policy for information security management? |  |  |
| **17** | ***Information security aspects of business continuity management*** | | | |
| **17.1** | **Information security continuity** | | | |
| 17.1.1 | Information security continuity | Defined policy for information security continuity? |  |  |
| **17.2**  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  YES  UNKNOWN  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO  NO | **Redundancies** | | | |
| 17.2.1 | Redundancies | Defined policy for redundancies? |  |  |
| **18** | ***Compliance*** | | | |
| **18.1** | **Compliance with legal and contractual requirements** | | | |
| 18.1.1 | Identification of applicable legislation and contractual requirement | Defined policy for identification of applicable legislation and contractual requirement? |  |  |
| 18.1.2 | Intellectual property rights | Defined policy for intellectual property rights? |  |  |
| 18.1.3 | Protection of records | Defined policy for protection of records? |  |  |
| 18.1.4 | Privacy and protection of personally identifiable information | Defined policy for privacy and protection of personally identifiable information? |  |  |
| 18.1.5 | Regulation of cryptographic control | Defined policy for regulation of cryptographic control? |  |  |
| **18.1** | **Independent review of information security** | | | |
| 18.1.1 | Compliance with security policies and standards | Defined policy for compliance with security policies and standards? |  |  |
| 18.1.2 | Technical compliance review | Defined policy for technical compliance review? |  |  |

|  |
| --- |
| **DISCLAIMER**  Any articles, templates, or information provided by Smartsheet on the website are for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk. |