**ISO 27002 INFORMATION SECURITY [](https://bit.ly/2Vodg53)  
GUIDELINES CHECKLIST TEMPLATE**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ISO 27001 CONTROL NUMBER** | **RANK** | **PRIORITY** | **OWNER** | **DATE ASSIGNED** | **DUE DATE** | **IN COMPLIANCE?** | **STATUS** | **NOTES** |
| **5. Security Policy Management** | | | | | | | | |
| 5.1 - Management has provided compliance direction and support? |  |  |  |  |  |  |  |  |
| **6. Corporate Security Management** | | | | | | | | |
| 6.1 - Internal information security task force has been established? |  |  |  |  |  |  |  |  |
| 6.2 - Measures in place to protect the org's mobile devices and network? |  |  |  |  |  |  |  |  |
| **7. Personnel Security Management** | | | | | | | | |
| 7.1 - Policy established for checking security prior to employment? |  |  |  |  |  |  |  |  |
| 7.2 - Policy established for security during employment? |  |  |  |  |  |  |  |  |
| 7.3 - Policy established  for security at termination? |  |  |  |  |  |  |  |  |
| **8. Organizational Asset Management** | | | | | | | | |
| 8.1 - Policy established for corporate assets? |  |  |  |  |  |  |  |  |
| 8.2 - Policy established for information classification method? |  |  |  |  |  |  |  |  |
| 8.3 - Policy established for controlling physical media? |  |  |  |  |  |  |  |  |
| **9. Information Access Management** | | | | | | | | |
| 9.1 - Policy established for information access management for business requirements? |  |  |  |  |  |  |  |  |
| 9.2 - Policy established for managing all users' access rights? |  |  |  |  |  |  |  |  |
| 9.3 - Policy established for user authentication? |  |  |  |  |  |  |  |  |
| 9.4 - Policy established  for controlling access to systems? |  |  |  |  |  |  |  |  |
| **10. Cryptography Policy Management** | | | | | | | | |
| 10.1 - Policy established  for control of the use of cryptographic controls and keys? |  |  |  |  |  |  |  |  |
| **11. Physical Security Management** | | | | | | | | |
| 11.1 - Policy established  for physical security management? |  |  |  |  |  |  |  |  |
| 11.2 - Policy established  for protecting the org's equipment? |  |  |  |  |  |  |  |  |
| **12. Operational Security Management** | | | | | | | | |
| 12.1 - Policy established  for operational security management procedures and responsibilities? |  |  |  |  |  |  |  |  |
| 12.2 - Policy established  for protecting the org from malware? |  |  |  |  |  |  |  |  |
| 12.3 - Policy established  for creating backup copies on a regular basis? |  |  |  |  |  |  |  |  |
| 12.4 - Policy established  for using logs to record security events? |  |  |  |  |  |  |  |  |
| 12.5 - Policy established  for controlling org's operational software? |  |  |  |  |  |  |  |  |
| 12.6 - Policy established  for addressing org's technical vulnerabilities? |  |  |  |  |  |  |  |  |
| 12.7 - Policy in place for minimizing impact of audit activities? |  |  |  |  |  |  |  |  |
| **13. Network Security Management** | | | | | | | | |
| 13.1 - Policy established  for protecting networks and facilities? |  |  |  |  |  |  |  |  |
| 13.2 - Policy established  for protecting information transfers? |  |  |  |  |  |  |  |  |
| **14. System Security Management** | | | | | | | | |
| 14.1 - Policy established  for ensuring security on inherent part of info systems? |  |  |  |  |  |  |  |  |
| 14.2 - Policy established  for protecting and controlling system development activities? |  |  |  |  |  |  |  |  |
| 14.3 - Policy established  for safeguarding data used for system-testing purposes? |  |  |  |  |  |  |  |  |
| **15. Supplier Relationship Management** | | | | | | | | |
| 15.1 - Policy established  for forming security agreements with suppliers? |  |  |  |  |  |  |  |  |
| 15.2 - Policy established  for managing suppliers' security and service deliveries? |  |  |  |  |  |  |  |  |
| **16. Security Incident Management** | | | | | | | | |
| 16.1 - Policy established  for identifying and responding to info security incidents? |  |  |  |  |  |  |  |  |
| **17. Security Continuity Management** | | | | | | | | |
| 17.1 - Policy established  for forming info security continuity controls? |  |  |  |  |  |  |  |  |
| 17.2 - Policy established  for redundancy builds for info-processing facilities? |  |  |  |  |  |  |  |  |
| **18. Security Compliance Management** | | | | | | | | |
| 18.1 - Policy established  for legal security requirements compliance? |  |  |  |  |  |  |  |  |
| 18.2 - Policy established  for executing security compliance reviews? |  |  |  |  |  |  |  |  |

**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.

This template is provided as a sample only. This template is in no way meant as legal or compliance advice. Users of the template must determine what information is necessary and needed to accomplish their objectives.