Distribution of the Information System's Modules and Common Security Controls

Posted on May 31, 2018

At the start of the risk assessment, there is a general statement about the information system that resembles its scope. However, that does not include the proper description of the information system. (National Institute of Standards and Technology [NIST], 2018)

The information system will be better described by a data flow diagram, description, or layout, which will assist in determining the key areas and requirements. Moreover, the detailed description of the information system will set the boundaries for the information security management system.

The information systems have not yet been registered with any office. However, the distribution of the information system's modules should be defined with their particular responsibilities. This document should be included in the security report. Through this information, organizations can perform activities related to information security more effectively.

RMF Step 2: Select Security Controls

Some areas of the HBWS's information system have security controls defined. These include the small hospital grant tracking system and Windows NT platforms. However, common security controls for networking components and remote login are undefined.

Common security controls should be carefully identified and monitored within the information systems. (NIST, 2020a, 2020b)

These newly identified security controls will assist the organization in identifying areas that need more security. These common security controls should be documented in the security plan.

There are a limited number of security controls mentioned before the common controls. These are not enough for strong information security management systems.

The identified and selected security controls should be mentioned in the security plan.

As fitting security controls have not been appropriately distinguished, no strategy to screen the security controls exists. An all-around archived arrangement for observing security controls recognizes regions where embraced controls might be excessively powerless or excessively prohibitive. This strategy ought to be incorporated into the security report of the security design.

A security plan has not been created for the association's data frameworks; hence, it can't be

surveyed. To decide on ampleness and pertinence, the administration or an administration-assigned party ought to undertake a normal and careful audit of the security plan. This audit should bring about conceivable upgrades or confirmation of the present security act and add it to the security report.

RMF Step 3: Implement Security Controls

The association is not currently actualizing any controls characterized by a security plan. Using controls that have been characterized and recorded inside a security plan enables the association to screen, survey, and enhance the chosen controls, which additionally secures the information systems. (NIST, 2018)

Should the picked controls be archived, the real utilization and execution ought to be reported in the security plan. This can guarantee that the controls are being completed effectively and give an underlying inspecting point for the control.

RMF Step 4: Assess Security Controls

Presently, there is no arrangement or technique for surveying the chosen security controls. This will give the association a guide to prepare for and complete an evaluation. (NIST, 2022)

The evaluation for the security control ought to be executed according to the evaluation plan. The evaluation will check whether the degree of security control has been secured during usage or not. Additionally, it is best to do the evaluation for the control ahead of schedule into the usage procedure so that any provisos, shortcomings, or vulnerabilities can be found and followed up on. This prevents any late disclosure of issues from causing a lot of rework for the group.

A security assessment report is created based on the yields of the security assessment process. This report is utilized to determine any shortcomings, vulnerabilities, and escape clauses in the security controls. When the report is displayed for the assessment of security controls, the data significant to the adequacy and vulnerability of security controls ought to be available in the report.

As examined before, the assessment report for the security controls will bring up the vulnerabilities and shortcomings. In view of the shortcomings recognized a plan for the remediation for the vulnerabilities should be distinguished and recorded. The remediation plan for various security controls is numerous or may not be the same, and when the remediation plan for the recognized vulnerabilities is characterized, it should detail the different advances that need to go for broke postured by the vulnerabilities. This remediation activity is utilized by the different framework proprietors, suppliers, and engineers as a guide. Likewise, one vital thing to note here is that this procedure should not be aimed at discovering issues. Rather, it ought to be an arrangement-situated process.

RMF Step 5: Authorize Information System

After restorative activities have been started in view of the security assessment, a plan to proceed or long-haul remediation is required. This is to guarantee the association follows a procedure to remedy or moderate all zones of worry from the assessment. The association has remedial activities prescribed in light of the underlying danger assessment, yet no plan to make a long-haul move. This documentation ought to be incorporated into the plan of activity.

The association has not particularly distinguished a mindful gathering to present the security bundle. This ought to be recorded inside the ISMS. This individual or gathering would then be able to utilize the security bundle, including the security report, assessment, and activity plan, to settle on instructed risk choices.

Risk is inborn with authoritative processes and methodology and should be appropriately decided and reported. This association needs to play out a nitty-gritty risk administration for the diverse techniques and available procedures. The risk administration procedure ought to be deliberately done, and the following ought to be secured: assessment, resistance, alleviation, and observation.

As specified before, the resilience level for all risks will likewise be reported. The resilience level for a risk decides the level to which the association is prepared to acknowledge that risk. AO will be the last specialist on whether the resistance level for the risk will be acknowledged or not. However, before AO considers this choice, he will take into account an assortment of variables.

RMF Step 6: Monitor Security Controls

The evaluations of changes that affect the information systems have not been completely done. Security consequences should be examined by the change management and added to the evaluation report of information security management systems. The negative consequences can be minimized due to underlying changes. (NIST, 2018)

Security controls should be regularly evaluated to confirm that they are in accordance with the information system’s requirements and organizational goals. However, the organization does not provide a policy to determine which group of security controls should be evaluated.

As the evaluation of current security controls is needed, similarly, the actions taken according to those evaluations should also be assessed. Sometimes, the evaluation of security controls can show that they are no longer needed by the organization. The corrective actions should be approved.

No, according to the results of ongoing monitoring, the organization has not revised or refreshed parts of its information security management systems. Maintaining the policy up to date ensures that security controls are also up to date and corrective actions are accurate. Hence, the reviewing

process is quick and effective.

The organization has not yet identified the officials-related security status reports, which results in ineffective completed reports. Appointing someone who is responsible for reviewing security reports can ensure the effectiveness of the corrective actions, monitor change activities, and provide other expertise in the field of information security.

Purpose:

COBIT is one of the most powerful structures compared to ISO 2002, NIST, and ITIL. It designs or plans major IT processes in a way that enables higher business management to profitably implement the rules, regulations, and procedures.

ITIL assists businesses in organizing IT resources and contributions by providing best practices to achieve the required goals.

ISO 27002 is a set of best practices for an information security implementation system. (International Organization for Standardization [ISO], 2022)

NIST is essential for the central bodies in the U.S. to ensure the conformity of security controls linked to national security.

Uses:

COBIT is used by business executives to exhibit major rules, regulations, and procedures.

ITIL is mostly used by the UK governing bodies.

ISO 27002 is used by the organizations' IT departments.

NIST is utilized by the U.S. government to achieve the ISMS needs.

Strengths:

COBIT is accepted worldwide, and it is managed by the Information Systems Audit and Control Association, which keeps it updated according to the latest technology.

ITIL is used by the UK government and is beneficial for U.K. companies. It increases efficiency and the economy by increasing visibility into and management of internal processes.

ISO 27002 enables the system managers to determine and resolve the gaps between communication and reporting.

NIST can be customized by any organization that intends to use this standard according to their business nature.

Weaknesses:

COBIT usually creates gaps in coverage.

ITIL lacks specific implementation details.

ISO 27002 is limited in scope as compared to other standards.

NIST is also limited in scope and can lead to gaps in coverage or reporting.

Certification and accreditation:

COBIT has four levels of certification:

1. Certified Information Systems Auditor Learn more about CISA (CISA)
2. Certified Information Security Manager Learn more about CISM (CISM)
3. Certified in the Governance of Enterprise IT (CGEIT)
4. Certified in Risk and Information Systems Control (CRISC)

ITIL has four certification levels: foundation, intermediate, expert, and master.

ISO 27002 is associated with the standard ISO 27001 and provides the certification for organizations.

NIST does not provide any certifications.

References

International Organization for Standardization. (2022). *ISO/IEC 27002:2022—Information security, cybersecurity and privacy protection: Information security controls*. https://www.iso.org/standard/75652.html

National Institute of Standards and Technology. (2018). *Risk Management Framework for information systems and organizations: A system life cycle approach for security and privacy* (Special Publication 800-37 Rev. 2). https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2020a). *Security and privacy controls for information systems and organizations* (Special Publication 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2020b). *Control baselines for information systems and organizations* (Special Publication 800-53B). https://doi.org/10.6028/NIST.SP.800-53B

National Institute of Standards and Technology. (2022). *Assessing security and privacy controls in information systems and organizations* (Special Publication 800-53A Rev. 5). https://doi.org/10.6028/NIST.SP.800-53Ar5