Kaden Salazar

Week 1 Reading Assignment 1

Information Assurance and Security CIS 563

Dr. Charles Butler

Points to Consider in Control Selection

Control selection requires balancing risk reduction with organizational constraints. Controls should be chosen to address specific risks and align with organizational objectives while integrating smoothly with existing safeguards. More precisely, there are four main points to consider when selecting controls, these are risk-based considerations, control objectives, constraints, and integration with existing controls.

1. Risk-based factors: Compare inherent and residual risk, ensuring controls reduce threats to an acceptable level (EC-Council, 2020). The degree of risk appetite guides how strong or extensive controls must be.
2. Control objectives: Controls may prevent, detect, deter, correct, recover, monitor, or raise awareness (International Organization for Standardization, 2022). Options include manual or automated, technical, or managerial (EC-Council, 2020).
3. Constraints: Evaluate time to deploy, cost vs. potential loss (Annualized Loss Expectancy), technical compatibility, operational impact, usability, cultural and ethical alignment, environmental factors, legal and compliance requirements, and staff availability (EC-Council, 2020; International Organization for Standardization, 2022).
4. Integration: New controls should complement existing ones. If infeasible, compensating controls may substitute when they meet the intent and rigor of the original requirement (EC-Council, 2020).

Implementation Process

The NIST Risk Management Framework (RMF) steps 4 through 7 provided structured steps for control implementation (Joint Task Force, 2018).

- Implement: Convert policies into safeguards through system configurations, access rules, and training. Assign responsibilities and document applications.
- Assess: Test effectiveness with vulnerability scans, penetration testing, configuration reviews, and audits.
- Authorize: Decision-makers review residual risk, assessment results, and remediation plans before approving or conditioning operation.
- Monitor: Continuously track control performance, evaluate new threats, and complete remediation activities to ensure ongoing effectiveness.

One of the main uses for controls is to bring risk to an acceptable level whenever it cannot be transferred or avoided. By selecting appropriate controls and implementing them effectively and efficiently, an organization is better able to safeguard assets, maintain compliance, support business objectives, and adapt to evolving threats.

References

EC-Council. (2020). *Certified Chief Information Security Officer (CCISO) Version 3 eBook Ed. 3* (3rd ed.). International Council of E-Commerce Consultants (EC Council). https://bookshelf.vitalsource.com/books/9781635673999

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks* (ISO Standard No. 27005:2022). https://www.iso.org/standard/80585.html

Joint Task Force. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2