Section 1: Week 3: Governance Provisions for Security Policy, Standards, and Procedure

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 7, 2020

North Central University

# Governance Provisions for Security Policy, Standards, and Procedure

## Information Security Lifecycle

The security lifecycle follows the Identify, Protect, Detect, Respond, and Recover stages (Sadgune & Dadgune, 2017). These stages reasonably align with the core feedback loop of ‘plan-do-act-check’ available in many Risk Management Frameworks (Radhakrishnan, 2015). Both follow the same precursor steps of enumerating threats against business artifacts and reducing that risk through protection schemes. After reducing risk, the processes diverge with the security lifecycle focusing on detecting and responding to infractions. Meanwhile, Risk Management, confirms the mitigations are appropriate and then seeks the next item from a prioritized list. However, not all risk management frameworks follow only the PDAC feedback loop and can extend the workflow to include more aspects of the security lifecycle. For instance, the NIST Cybersecurity Framework explicitly includes each guidance for each stage of the security lifecycle (Grohmann, 2018).

## Components of Risk Management Strategy

Table 1: Artifacts of Risk Management Strategy

|  |  |  |
| --- | --- | --- |
| Name | Description | Examples |
| Policies | Set the high-level expectations of approach (Compliance Forge, u.d.) | Data must be encrypted in transit and at rest Employees should not reuse passwords |
| Guidelines | The cultural norms that justify our actions (Weston, Conklin, & Drobnis, 2018) | If you see something, say something Avoid unlicensed contractors unless necessary |
| Standard Operating Procedures | A checklist that enumerates steps to arrive at a desirable outcome (BizManualz, u.d.) | Process for adding or removing a user Process for deploying service updates |
| Baselines | Minimum acceptable criteria for work acceptance | Performance and reliability SLA |

Risk Management Strategies tend to be hierarchical with the root nodes consisting of generic themes. At the lower levels of the tree, ideas become less abstract and read more as process decisions. Since the leaves provide the implementation details to support their parent branches, team members can focus on the layer most relevant to their role. If the executive leadership team needs to monitor every minor detail of the implementation, then it would be challenging to deliver efficiently across larger enterprises.

## Ideal Risk Management Framework

Choosing the right framework requires assessing the needs of flexibility and regulatory requirements. When the organization lacks consistent or mature processes, then the NIST Cybersecurity framework can be an ideal choice because of the highly adaptive design (Grohmann, 2018). Businesses use NIST’s guidelines to determine which aspects of the management lifecycle are “good, better, or best” and then prioritize future improvements. In contrast, more rigid solutions like ISO27000 require significant cultural shifts and can encounter political pressure to fail.

Table 2: Risk Management Frameworks

|  |  |  |
| --- | --- | --- |
| Name | Description | Ideal Environment |
| National Institute of Standards and Technology (NIST) Cybersecurity Framework (Grohmann, 2018) | Flexible methodology to approach controls and evolve them over time | Large enterprise and businesses with varying levels of process maturity |
| International Organizational Standards (ISO) 27000 (Gillies, 2011) | Rigid set of requirements for ensuring appropriate controls | Small enterprises and heavily regulated industries |
| Control Objectives for Information and Information related Technology (COBIT) (Devos & Van de Ginste, 2015) | Collection of industry best practices and guidelines | Organizations that need a middle ground between NIST and ISO frameworks |

## Policy Hierarchy, Components, and Tooling

The policies of the risk management strategy need to identify threats to business artifacts from both negligence and malicious behavior (Mickens, 2015). For instance, erroneous system commands should limit the blast radius by default. Reducing the potential impact requires capabilities that build on top of authentication, authorization, and auditing (AAA). Alice is allowed to send documents to the network printer, but should she be permitted to request a single 10,000-page document? Quota management scenarios reoccur at all levels of business processes to block these erroneous actions.

Another collection of policies center around ensuring the confidentiality, integrity, and availability (CIA) of the institution. For instance, customer data needs to encrypted in transit and at rest. When systems are negligent, and customer privacy is compromised, then litigation and public relations risk come into the picture. These challenges create the necessary incentives for businesses to be mindful and prioritize the safe handling of data. Similar characteristics occur with integrity, such as tampering attacks leading to repudiation scenarios. Lastly, data that is unavailable cannot assist with decision processes and is therefore useless. Policies need all aspects of the data’s CIA.

Proper tooling can make or break the successful adoption of a risk management strategy. When users find a specific policy or practice to inconvenient, then they pursue solutions to minimize that friction (Busby, Green, & Hutchison, 2017). For example, a policy that asks all employees to sign and encrypt their email is unlikely to be sustainable if they need to execute complex commands from the terminal window. Meanwhile, the same policy with a simple button to “send with encryption,” will meet less resistance because it does not increase the workflow. Other scenarios also exist with firewalls and monitoring systems that need to do the ‘right thing by default.’ Policymakers must remember that the objective of security and risk management is to aid the business in its mission (Dai Zovi, 2019). The inverse solution is not sustainable and will be riffle with political opposition.

# References

BizManualz. (u.d.). *What is a Standard Operating Procedure (SOP)*? Retrieved June 21, 2020, from BizManualz: https://www.bizmanualz.com/save-time-writing-procedures/what-are-policies-and-procedures-sop.html

Busby, J., Green, B., & Hutchison, D. (2017). Analysis of Affordance, Time, and Adaptation in the Assessment of Industrial Control System Cybersecurity Risk. *Risk Analysis: An International Journal, 37*(7), 1298-1314. doi:https://doi-org.proxy1.ncu.edu/10.1111/risa.12681

Compliance Forge. (u.d.). *Policy vs. Standard Operating Procedure vs. Control vs. Procedure*. Retrieved June 21, 2020, from Compliance Forge: https://www.complianceforge.com/word-crimes/policy-vs-standard-vs-control-vs-procedure

Dai Zovi, D. (2019). Every Security Team is a Software Team Now. *Black Hat USA.* Las Vegas, NV, USA: Black Hat. Retrieved May 9, 2020, from https://www.youtube.com/watch?v=8armE3Wz0jk

Devos, J., & Van de Ginste, K. (2015). Towards a Theoretical Foundation of IT Governance - The COBIT 5 case. *Electronic Journal of Information Systems Evaluation, 18*(2). Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=edb&AN=109261833&site=eds-live

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM Journal, 23*(4), 367-376. doi:http://dx.doi.org.proxy1.ncu.edu/10.1108/17542731111139455

Grohmann, A. (2018). Evolution of the cybersecurity framework. *ISSA Journal, 16*(7), 14-18. Retrieved May 2, 2020, from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=tsh&AN=130572679&site=eds-live

Mickens, J. (2015, September 9). *Not Even Close, The State of Computer Security with Slides*. Retrieved May 24, 2020, from YouTube: https://youtu.be/tF24WHumvIc

Radhakrishnan, S. (2015). COBIT Helps Organizations Meet Performance and Compliance Requirements. *COBIT Focus, 5*, 1-5. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=bth&AN=102026122&site=eds-live

Sadgune, R., & Dadgune, A. (2017, June 11). *Cyber Security Lifecycle*. Retrieved June 21, 2020, from HackForLab: https://hackforlab.com/cyber-security-lifecycle/

Weston, H., Conklin, T., & Drobnis, K. (2018). Assessing and resetting culture in enterprise risk management. *Assurances et Gestion Des Risques, 85*(1), 131-166. doi:https://doi-org.proxy1.ncu.edu/10.7202/1051319ar