A Strategic Risk-Based Approach to Systems Security Engineering

In the 21st century, the backbones of business, trade, economy and critical infrastructure for public- and private-sector enterprises are information systems and the data they store, process and transmit. The ubiquity associated with the modern computing environment, which includes the Internet of Things (IoT), cloud and virtualization, adds to the complexity of these systems. As technology continues to expand and new information systems emerge, enterprises must consider how to protect their information and achieve their mission and business objectives.

When enterprises engineer and deploy new information systems, they must do so in secure ways. Traditionally, many enterprises used compliance-based approaches to ensure the security of new systems. However, security requirements for information systems may differ significantly based on industry, geographic location, types of information processed, and the laws and regulations governing minimum compliance requirements. Therefore, enterprises may find that a risk-based approach to systems security engineering is a better way to address the ever-evolving threat landscape while also maintaining strategic alignment with business goals and objectives.

Cybersecurity Risk Overview

Before an enterprise engages in a system engineering endeavor, it must identify and assess risk using an integrated approach to address security protection needs in emerging systems. There are many different kinds of risk, including business, legal, regulatory, financial, operational and reputational risk. These risk categories may have a direct or indirect connection to cybersecurity risk, which involves the unauthorized disclosure, alteration or unavailability of system resources or information. Cybersecurity risk is typically a measure of the likelihood of an adverse event occurring and the impact if it does.[1] Identifying and assessing cybersecurity risk during systems engineering efforts is crucial, but it is meaningless without defining the context in which risk response decisions occur.

Prior to risk identification, enterprises should establish their risk capacity and risk appetite. Risk appetite is the allocation of risk capacity for various types of risk—that is, the amount of risk an enterprise is willing to accept in pursuit of its mission and business objectives.[2] Enterprises that fail to define their risk appetite may be faced with making *ad hoc*, chaotic decisions, leading to misaligned priorities, responses and funds. Establishing a risk appetite allows risk owners to be held accountable when risk exceeds risk appetite.[3]

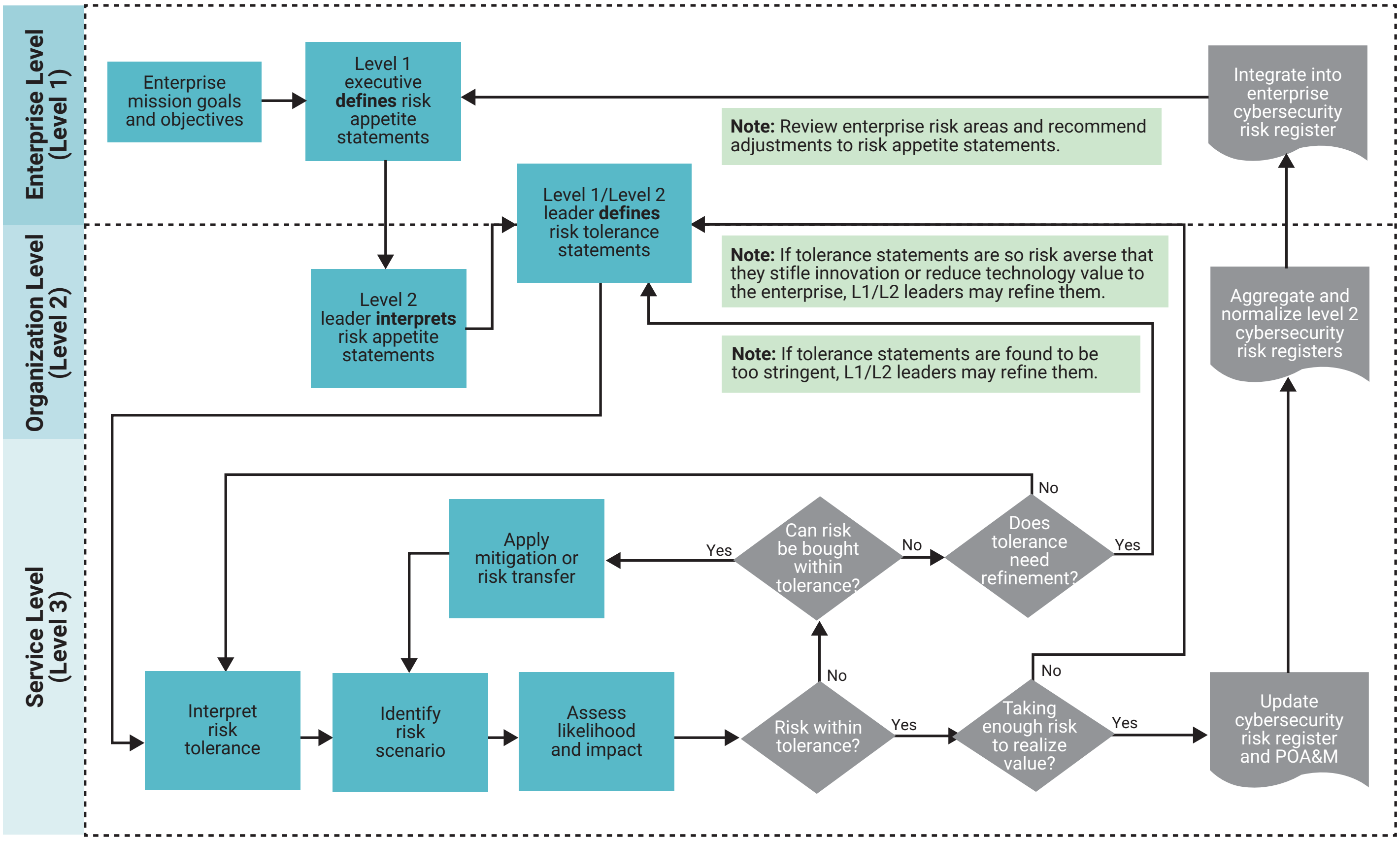
Once risk appetite has been defined, enterprises must determine their risk tolerance (**figure 1**). The US National Institute of Standards and Technology (NIST) defines risk tolerance as “The level of risk or degree of uncertainty that is acceptable to organizations and is a key element of the organizational risk frame.”[4] Adequate cybersecurity risk management ensures that risk is aligned with the enterprise’s risk appetite and tolerance levels to achieve cost-effectiveness.[5]

HUNTER SEKARA | CISA, CRISC, CISM, CISSP

Is a lead information system security officer for SiloSmashers, Inc. He works closely with enterprise executives and stakeholders to achieve business objectives in a secure manner.

FIGURE 1

Example Risk Appetite and Risk Tolerance Process Flow


Enterprise Level (Level 1)
Organization Level (Level 2)
Service Level (Level 3)
Enterprise mission goals and objectives
Level 1 executive **defines** risk appetite statements
Integrate into enterprise cybersecurity risk register
Note: Review enterprise risk areas and recommend adjustments to risk appetite statements.
Level 1/Level 2 leader **defines** risk tolerance statements
Level 2 leader **interprets** risk appetite statements
Note: If tolerance statements are so risk averse that they stifle innovation or reduce technology value to the enterprise, L1/L2 leaders may refine them.
Note: If tolerance statements are found to be too stringent, L1/L2 leaders may refine them.
Aggregate and normalize level 2 cybersecurity risk registers
Apply mitigation or risk transfer
Yes
Can risk be bought within tolerance?
No
Does tolerance need refinement?
Yes
No
Interpret risk tolerance
Identify risk scenario
Assess likelihood and impact
Risk within tolerance?
No
Yes
Taking enough risk to realize value?
No
Yes
Update cybersecurity risk register and POA&M

Source: Quinn, S.; N. Ivy; M. Barrett; L. Feldman; G. Witte; R. K. Gardner; National Institute of Standards and Technology Internal Report 8286A *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*, USA, 2021, *https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8286A.pdf.* Reprinted with permission.

Risk Assessment for Systems Engineering

Enterprises are faced with various threats that may seek to harm assets and operations, including information, information systems, facilities and personnel. Before risk factors can be identified, enterprises must identify the assets they are trying to protect and the value of those assets and the services they provide.[6] This context-aware approach to security ensures that new systems include cost-effective security measures proportionate to asset value, probability of occurrence and potential magnitude of loss. There are many different categories of assets; however, from a cybersecurity perspective, assets usually consist of information and information systems. To be effective, asset identification must include relevant stakeholders with a solid understanding of the asset's impact and protection needs.[7]

One method of identifying assets early on is to conduct a business impact analysis (BIA). With a BIA, an enterprise can document mission and business functions for its information system and the assets that support each mission and business function and the value of services delivered.[8] The BIA provides direct traceability between the system's intended mission and business functions and the supporting technical components. It can also identify potential adverse impacts that may result from a realized risk. The BIA output results in a prioritized list of mission and business functions and the supporting systems and components.[9] The public sector in the United States relies on US Federal Information Processing Standard (FIPS) 199 for asset identification and valuation. Whereas a BIA values information based on availability, FIPS 199 also considers confidentiality and integrity. With FIPS 199, once an asset has been identified, it is given a provisional value, based on the type of information and the impact level, as defined by NIST Special Publication (SP) 800-60. Impact levels and categorization provide input into the definition of security requirements.[10] The BIA and FIPS 199 methods can be used in tandem to develop a solid baseline of assets and values.

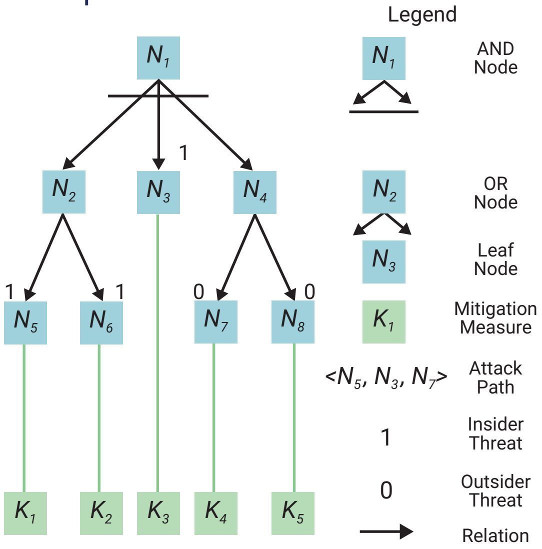
Threat Identification

The growing number of security threats can present complex challenges to the engineers responsible for designing security measures.[11] Enterprises must apply an engineering focus in the early phases of system design, rather than relying on technology-centric solutions to address security threats after system deployment. One such approach is threat modeling.

Threat modeling enables system and software engineering professionals to compile a system's threat profile by analyzing it through the lens of a malicious actor and then identifying potential cybersecurity risk factors.[12] Threat models display threats using tree structures and/or relationships (**figure 2**).[13]

FIGURE 2

Example Tree Structure



Source: Li, X.; K. He; Z. Feng; G. Xu; "Unified Threat Model for Analyzing and Evaluating Software Threats," *Security Communication Networks*, vol. 7, 2014, *https://doi.org/10.1002/sec.599*. Reprinted with permission.

These tree structures represent the attack paths a malicious actor would use to compromise the system.[14] A standard method of identifying threats is the STRIDE model.[15] STRIDE is a threat model that categorizes threats as spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privileges.[16] STRIDE allows for threat identification relating to someone impersonating another's identity (spoofing), unauthorized modification of information or systems (tampering), false claims that an individual was not responsible for an action (repudiation), revealing information to unauthorized parties (information disclosure), interrupting timely access to information or systems (denial of service), and someone being granted access to perform an action in which they are not authorized (elevation of privileges). Once threats have been identified, security professionals perform threat-risk ranking using the DREAD model.[17] DREAD is a threat-risk ranking model that is used to calculate a risk score based on damage, reproducibility, exploitability, affected users and discoverability.[18] DREAD allows for the ranking of threats based on the adverse impact of the threat event (damage), the ease of recreating the threat event (reproducibility), the ease of exploitation (exploitability), the number of individuals that will be impacted (affected users) and how easy it is to find the weakness to exploit (discoverability). Based on the results, enterprises can define, plan and implement security controls to promote resilient, secure systems.[19]

> "Enterprises should use a variety of vulnerability assessment techniques to identify weaknesses during systems engineering."

Vulnerability Identification

Traditionally, system development efforts have focused on functionality rather than quality or security.[20] This approach raises concerns because adversaries are continually looking for exploitable vulnerabilities. To remain vigilant and adapt to the ever-evolving threat landscape, enterprises must identify vulnerabilities not only in information systems, but also in processes, procedures and people. During engineering efforts, both systems comprising commercial off-the-shelf components and those using custom-developed components may harbor known and unknown vulnerabilities.[21] Vulnerabilities can be introduced not only intentionally by adversaries, but also through the supply chain. However, it is vital

LOOKING FOR MORE?

- Read *Risk IT Framework. www.isaca.org/risk-it-f2*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

to note that many vulnerabilities introduced in the early phases of system development result from architectural and design flaws.[22]

> "Once security controls have been designed, they should be implemented in accordance with the planned risk responses."

Enterprises should use a variety of vulnerability assessment techniques to identify weaknesses during systems engineering. These techniques include static application security testing (SAST), dynamic application security testing (DAST), vulnerability scanning and penetration testing.[23] In addition, vulnerability detection can be performed via configuration scanning using automation such as Security Content Automation Protocol (SCAP) and Open Vulnerability and Assessment Language (OVAL).[24] A plethora of guidance is available through resources such as the NIST National Vulnerability Database (NVD), MITRE Common Vulnerabilities and Exposures (CVE) and Common Weaknesses Enumeration (CWE), and the Open Web Application Security Project (OWASP). Enterprises should exercise caution when relying solely on the Common Vulnerability Scoring System (CVSS) because predisposing conditions may increase or decrease vulnerability. These predisposing conditions may include information-related, technical, environmental or operational conditions.[25]

Risk Determination

After identifying threats and vulnerabilities, the next step is to determine the likelihood of an adverse event occurring and the potential impact on the enterprise. Enterprises should ask:

- Are there threats?
- What are their capabilities?
- What is their intent?
- Will there be an impact?

An adequate risk analysis is crucial to ensure that the appropriate levels of security are integrated into system requirements, commensurate with asset value and risk. A risk analysis can also determine how funds should be spent.[26] This cost-effective approach to systems engineering ensures that systems are neither oversecured nor undersecured while also properly allocating time and resources during planning, design and implementation. The early integration of security into system development maximizes stakeholder investments and reduces the cost of security control implementation.[27]

Selecting and Planning Risk Responses

The risk assessment results in a list of risk factors related to the system, processes and enterprise, providing input into the definition of security requirements. The enterprise can then rank the risk factors in order of criticality to prioritize funding and resources, concentrating on areas with the highest probability of threat and the greatest possible impacts. Risk responses should be selected based on cost-benefit principles, taking into consideration the risk vs. economic trade-offs. Performing a cost-benefit analysis is prudent to verify that the costs of security implementations are not higher than the costs associated with a lack of security controls.[28] A cost-benefit analysis also influences the decision-making process regarding the appropriate risk response: acceptance, mitigation, transfer or avoidance. Once a risk response is selected, it must be prioritized. For example, how soon is action needed? If the enterprise chooses risk acceptance, no further action is required. But if the enterprise chooses risk avoidance, it must decide how abruptly to remove the affected system component, function or process associated with the risk. Incorrect prioritization of responses can, ultimately, lead to a reduction in business value and the failure of secure system deployment.[29]

Once a risk response decision has been made, the enterprise must determine which responsible entities will be involved in the response. These responsible entities may include executives, program managers, engineers, suppliers, third-party vendors or insurance enterprises. Once responsibilities are determined, they must be clearly communicated. A requirements traceability matrix; system security plan; risk treatment plan; and responsible, accountable, consulted, informed (RACI) matrix are practical tools for communicating security responsibilities.

Effective risk responses require adequate planning. If risk mitigation is selected, each responsible party must research, design and plan the security controls to be implemented, considering assumptions, constraints and feasibility. Enterprises may seek to leverage industry best practices such as Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) benchmarks or even vendor security documentation for technical-related controls. An independent party should review planned risk responses for quality, effectiveness and value prior to implementation.

Security Implementation

Once security controls have been designed, they should be implemented in accordance with the planned risk responses. By documenting the security design, security plans and other requirements, enterprises can guide the implementation of cost-effective, risk-based security measures while maintaining traceability with risk assessment results.[30] During the implementation of security controls, risk documentation must be updated continuously because it might not be feasible to implement the security controls as initially designed.[31] Complications may occur due to technical limitations, lack of resources or funding issues. Therefore, it is critical to identify, document and communicate any deviations from the planned risk responses and identify alternative security measures and compensating controls.

> "When compliance is the primary driver of system security engineering efforts, gaps are likely to form between security objectives and mission and business objectives."

During implementation, a verification and validation (V&V) team should test the effectiveness of security controls to ensure that they are adequate.[32] V&V is a systems engineering principle that helps improve quality of software using a combination of testing methodologies to ensure software performs its intended functions and that it performs them correctly.[33] This objective-based approach ensures that the system meets specified requirements and achieves mission and business objectives while staying within the degree of risk tolerance.[34] Security testing may include a combination of assessment procedures, using both automated mechanisms and manual inspections. The depth and rigor of security testing should be based on security assurance requirements set forth by the enterprise.[35] The results of security testing should provide evidence of the effectiveness of security controls.

Conclusion

Once a system is deployed and enters the operation and maintenance phase, security cannot be ignored. As a system evolves throughout its life cycle, it must be monitored and managed to keep risk at an acceptable level. Enterprises should consider defining key risk indicators (KRI) to monitor and alert risk owners of emerging risk. Continuous risk monitoring is critical because compliance with regulations does not guarantee the success of security objectives.[36] When compliance is the primary driver of system security engineering efforts, gaps are likely to form between security objectives and mission and business objectives. Given the costs and reputational damage associated with cyberattacks, enterprises must identify cybersecurity risk and allocate security controls at the earliest stages of the system's life cycle.

Before systems engineering efforts begin, enterprises should develop a cybersecurity risk strategy, outlining the appropriate methodologies, definitions and approach to cybersecurity risk management to ensure alignment with the enterprise's overall risk management strategy. Given the potential adverse impacts resulting from cyberthreats, a holistic methodology to address cybersecurity risk management can help enterprises standardize their approach to risk identification, analysis, prioritization and response, and align systems engineering efforts with strategic objectives. Enterprises that take an integrated approach to cybersecurity risk management and systems engineering are better prepared to develop secure, trusted and resilient systems.

Endnotes

1 National Institute of Standards and Technology (NIST), Special Publication (SP) 800-30, Rev. 1, *Guide for Conducting Risk Assessments*, USA, 2012, *https://doi.org/10.6028/NIST.SP.800-30r1*

2 Duncan, B.; Y. Zhao; M. R. Whittington; "Corporate Governance, Risk Appetite and Cloud Security Risk: A Little Known Paradox. How Do We Square the Circle?" Aberdeen University Research Archive (AURA), Scotland, 2017, *https://aura.abdn.ac.uk/bitstream/handle/2164/8673/08CloudRiskCR.pdf?sequence=1&isAllowed=y*

3 Pareek, M.; "What Is Your Risk Appetite?" *ISACA® Journal,* vol. 4, 2013, *https://www.isaca.org/archives*

4 National Institute of Standards and Technology SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, USA, 2011, *https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=908030*

5 Stine, K.; S. Quinn; G. Witte; R. Gardner; *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, National Institute of Standards and Technology Interagency Internal Report, USA, 2020, *https://doi.org/10.6028/NIST.IR.8286*

6 Kure, H.; S. Islam; M. A. Razzaque; "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System," *Applied Sciences*, vol. 8, 2018, *https://doi.org/10.3390/app8060898*

7 Kure, H.; S. Islam; "An Assets Focus Risk Management Framework for Critical Infrastructure Cyber Security Risk Management," *IET Cyber-Physical Systems: Theory and Applications*, vol. 4, 2019, *https://doi.org/10.1049/iet-cps.2018.5079*

8 Torabi, S. A.; H. Soufi; N. Sahebjamnia; "A New Framework for Business Impact Analysis in Business Continuity Management (With a Case Study)," *Safety Science*, vol. 68, 2014, p. 309–323, *https://doi.org/10.1016/j.ssci.2014.04.017*

9 Swanson, M.; P. Bowen; A. Phillips; D. Gallup; D. Lynes; National Institute of Standards and Technology SP 80-43, Rev. 1, *Contingency Planning Guide for Federal Information Systems,* USA, 2010, *https://doi.org/10.6028/NIST.SP.800-34r1*

10 Stine, K.; R. Kissel; W. Barker; J. Fahlsing; J. Gulick; National Institute of Standards and Technology SP 800-60, Vol. 1, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories,* NIST, 2008, *https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final*

11 Abdul Karim, N.; A. Albuolayan; T. Saba; A. Rehman; "The Practice of Secure Software Development in SDLC: An Investigation Through Existing Model and a Case Study," *Security and Communication Networks*, vol. 9, 2016, *https://doi.org/10.1002/sec.1700*

12 Marback, A.; H. Do; K. He; S. Kondamarri; D. Xu; "A Threat Model-Based Approach to Security Testing," *Software: Practice and Experience*, vol. 43, 2013, *https://doi.org/10.1002/spe.2111*

13 Li, X.; K. He; Z. Feng; G. Xu; "Unified Threat Model for Analyzing and Evaluating Software Threats," *Security Communication Networks*, vol. 7, 2014, p. 1454–1466, *https://doi.org/10.1002/sec.599*

14 *Op cit* Marback *et al.*

15 Guan, H.; W. R. Chen; H. Li; J. Wang; "STRIDE-Based Risk Assessment for Web Application," *Applied Mechanics and Materials*, vol. 58–60, 2011, p. 1323–1328, *https://doi.org/10.4028/www.scientific.net/amm.58-60.1323*

16 Thompson, D. R.; J. Di; M. K. Daugherty; "Teaching RFID Information Systems Security," *IEEE Transactions on Education*, vol. 57, iss. 1, 2014, *https://ieeexplore.ieee.org/document/6524969/authors#authors*

17 Omotosho, A.; B. Haruna; O. Olayemi Mikail; "Threat Modeling of Internet of Things Health Devices," *Journal of Applied Security Research*, vol. 14, 2019, p. 1–16, *https://doi.org/10.1080/19361610.2019.1545278*

18 Ingalsbe, J.; L. Kunimatsu; T. Baeten; N. R. Mead; "Threat Modeling: Diving Into the Deep End," *IEEE Software,* vol. 25, iss. 1, 2008

19 *Op cit* Li *et al.*

20 de Vicente, M.; B. Higuera; S. Montalvo; "The Application of a New Secure Software Development Life Cycle (S-SDLC) With Agile Methodologies," *Electronics*, vol. 8, iss. 11, 2019, p. 1218, *https://doi.org/10.3390/electronics8111218*

21 Pachariya, M. K.; A. Sharma; "An Integrated Framework for Software Vulnerability Detection, Analysis and Mitigation: An Autonomic System," *Sādhanā*, vol. 42, 2017, p. 1–13, *https://doi.org/10.1007/s12046-017-0696-7*

22 Horton, S.; "Are Software Security Issues a Result of Flaws in Software Development Methodologies?" ProQuest Dissertations and Theses, 2020, *https://www.proquest.com/dissertations-theses/are-software-security-issues-result-flaws/docview/2405158801/se-2?accountid=8289*

23 Tudela, F. M.; J.-R. B. Higuera; J. B. Higuera; J.-A. S. Montalvo; M. I. Argyros; “On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications,” *Applied Sciences,* vol. 10, iss. 24, 2020, *https://doi.org/10.3390/app10249119*

24 Waltermire, D.; S. Quinn; H. Booth; K. Scarfone; D. Prisaca; National Institute of Standards and Technology SP 800-126, Rev. 3, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3*, USA, 2018, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf*

25 *Op cit* NIST SP 800-30

26 Hein, D.; H. Saiedian; “Secure Software Engineering: Learning From the Past to Address Future Challenges,” *Information Security Journal: A Global Perspective*, vol. 18, 2009, p. 8–25, *https://doi.org/10.1080/19393550802623206*

27 Kumar, R.; K. Mustafa; “Security Requirements Development Framework (SRDF),” *International Journal of Advanced Research in Computer Science*, vol. 2, iss. 5, 2011, *https://www.proquest.com/scholarly-journals/security-requirements-development-framework-srdf/docview/1443710870/se-2*

28 Olifer, D.; N. Goranin; A. Kaceniauskas; A. Cenys; “Controls-Based Approach for Evaluation of Information Security Standards Implementation Costs,” *Technological and Economic Development of Economy*, vol. 23, iss. 1, 2017, p. 196–219, *https://doi.org/10.3846/20294913.2017.1280558*

29 Naicker, N.; M. Maharaj; “Investigating Agile Requirements Engineering Practices in the South African Software Development Market,” *Journal of Computing and Information Technology*, vol. 28, 2020, p. 33–58, *https://doi.org/10.20532/cit.2020.1004868*

30 National Institute of Standards and Technology SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, USA, 2018, *https://doi.org/10.6028/NIST.SP.800-37r2*

31 *Ibid.*

32 Park, J.; Y. Suh; “A Development Framework for Software Security in Nuclear Safety Systems: Integrating Secure Development and System Security Activities,” *Nuclear Engineering and Technology,* vol. 46, 2014, p. 47–54, *https://doi.org/10.5516/NET.04.2012.061*

33 Wallace, D. R.; R. U. Fujii; “Software Verification and Validation: An Overview,” *IEEE Software,* vol. 6, iss. 3, 1989, *https://www.proquest.com/scholarly-journals/software-verification-validation-overview/docview/215835583/se-2?accountid=8289*

34 Ross, R.; M. McEvilley; J. Oren; National Institute of Standards and Technology SP 800-160, Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, USA, 2016, *https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=922194*

35 National Institute of Standards and Technology SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, USA, 2014, *https://doi.org/10.6028/NIST.SP.800-53Ar4*

36 Albuquerque, R.; L. Villalba; A. Sandoval Orozco; F. Buiati; T-H. Kim; “A Layered Trust Information Security Architecture,” *Sensors*, vol. 14, 2014, p. 22754–22772, *https://doi.org/10.3390/s141222754*