Risk-based recommendations form the basis of secure and resilient organizational decision-making, and particularly in today's evolving threat landscape organizations must rely on structured tools, processes and reliable resources in order to evaluate risk in a manner that is repeatable, defensible, data-driven and evidence-based. There are multiple tools which assist in this endeavor such as Risk Registers, Business Impact Analyses, vulnerability management tools, as well as reputable compliance frameworks, all of which result in decision-making that protects systems, processes, people and operational sustainability.

Using Tools to Make Risk-Informed Recommendations:

Tools enable decision-makers to quantify, and prioritize, threats in order to ensure that recommendations are based on actual measurable evidence instead of assumptions which can be influenced by individual bias and there is a wide array of tools available to utilize. Risk Registers are one of the primary tools for this purpose; documenting the risks, likelihood of a risk being actualized, the potential impacts as a result of that actualization, the cost to mitigate or remediate, and controls that can be used to mitigate risks (Peacock, J., n.d.). Risk Registers can utilize Common Vulnerability Scoring System (CVSS) scores, which are not a measure of risk but can be used to assign a specific likelihood and impact rating (NIST, 2024.), and by using the CVSS's qualitative measure of a vulnerabilities severity and understanding of the value of assets, Analysts can create a direct justification for recommendations for patching, network isolation, or other techniques to protect systems and data.

A Business Impact Analysis (BIA) is another important tool which upholds risk-informed decisions by clearly identifying critical business functions, establishing specific metrics surrounding Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) and

Maximum Tolerable Downtime (MTD), all of which provide guidance on acceptable timelines for processes or systems to be returned to full operation after a disruption. (NIST, 2010.) For example, if a fintech BIA outlines that a core transaction system must recover within 30 minutes in order to avoid major revenue losses, this dictates that recommendations address some form of failover or redundant systems in place for business continuity and these recommendations are based on evidence aligned with operational priorities, not simply a suggestion born of intuition.

There are several other tools which all can be used in a layered manner in conjunction with each other to assist with upholding business continuity, such as vulnerability management platforms, as well as monitoring tools such as a SIEM application. Vulnerability management tools, such as OpenVAS, help to correlate vulnerabilities with real business assets, in order to provide precise recommendations in terms of prioritization and without that context it's possible that recommendations may be misaligned with true exposure leading to delays in recovery, or an inefficient order of systems recovery. OpenVAS identifies misconfigurations, outdated software, and even weak passwords which can be exploited, classifies the system resources and can eliminate vulnerabilities on a priority basis (Geeks for Geeks, 2025). When used with SIEM tools, such as Splunk, which are efficient at aggregating log data and creating alerts for anomalous behavior, an Analyst can be certain that recommendations are anchored in accurate, real-time, measurable data to improve decision quality and overall resilience.

An example of utilizing tools, or in this case the impact of not utilizing tools, is the 2013 Target breach, because SIEM log correlation could have assisted in creating a risk-informed recommendation to segment the HVAC vendor's network segment **before** attackers were able to abuse credentials and gain access to the primary network. Utilizing SIEM triage rules and asset-

based risk scoring, Target could have justified the recommendation by showing a high likelihood of exploit, combined with a significant business impact if that vulnerability was realized. Post-breach, Target did invest heavily in tools such as SIEM solutions, network segmentation and vendor risk management (Framework Security, 2025).

Using Resources to Make Risk-Informed Recommendations:

Utilizing frameworks and resources helps to support continual improvements post-breach incidents, in the event risk mitigation is not sufficient and there is a successful exploit. There are multiple authoritative and reputable resources which help provide frameworks and structure to risk-informed recommendations in order to ensure that decisions align with broadly accepted best practices and some examples of these frameworks are the NIST Cybersecurity Framework (CSF) and the CIS Critical Security Controls. These frameworks provide standardized guidance and act as guidelines to help Analysts justify why specific controls are required and how they are prioritized, to protect an organization's assets, systems, and data. The NIST CSF provides guidance to manage cybersecurity risks and includes functions, categories and subcategories with 6 core functions; govern, identify, protect, respond, and recover to organize cybersecurity outcomes at their highest level (NIST, 2024).

The CIS Controls are a prescriptive and prioritized set of best practices used to strengthen cybersecurity posture to ensure organizations comply with industry regulations, simplify their approach to threat protection, and achieve essential cyber hygiene (CIS, n.d.). These frameworks help create clear justifications of risk recommendations and allow organizations to avoid ad-hoc decisions, instead relying on structured foundations that have been vetted by practitioners across

the world and ensure the organization aligns with compliance expectations to ensure recommendations are consistent and defensible.

An example of utilizing these frameworks is using CIS Controls to assess and prioritize cybersecurity controls within an organization by leveraging CIS Control 8; Audit Log Management, and CIS Control 9; Email and Web Browser Protections, as resources to spot weaknesses in logging and phishing vulnerabilities. Using this assessment, the organization can create risk-informed recommendations to implement a centralized SIEM for log correlation, in conjunction with adding an email filtering solution to reduce phishing risks, and these recommendations are grounded in industry-backed best practices but still tailored to the organization's specific risk profile (CIS, n.d.).

Identifying and Minimizing Bias in Risk-Informed Recommendations:

Bias can undermine decision quality in multiple ways; by skewing perception of the likelihood of a risk, the potential impact of a risk, or even the prioritization of risks, all of which can lead to poor outcomes. There are a wide array of cognitive biases, all of which distort risk management decisions and some of them are; the reflection effect, isolation effect, nonlinear preferences, and conjunction fallacy. Reflection effect is when facing a potential loss, a decision-maker may paradoxically prefer risky gambles as opposed to confirmed smaller losses and in security this may make risk professionals gamble on costly mitigations which might fail, instead of accepting controlled and predictable losses (Wit, J. & Meyer, C., 2022).

In order to minimize these biases, it is imperative that risk-informed recommendations incorporate the structured decision-making frameworks we discussed; CIS Controls and NIST CSF and Analysts must utilize objective data analysis when considering decisions. Incorporating

diverse perspectives from multiple contributors is also a key factor in bias minimization, while leveraging quantitative risk assessment tools further reduces potential distortions due to bias, which improves overall decision quality by employing mathematical models to quantify risks based on their impact and likelihood, not based on anecdotal evidence or past experiences, etc. (Scrut Automation, 2025).

Utilizing a Systems Thinking Approach:

Risks do not exist in isolation, but rather are typically present when there are interdependencies in play and systems thinking requires a comprehensive understanding of how risk recommendations impact people, technology, and processes as a whole. An example would be the required implementation of Multi-Factor Authentication (MFA), which improves security posture and credential protection but can also cause user experience interruptions and frustration to users and require user training at rollout which impacts the people aspect of an organization, while processes are also impacted in regards to modifying existing workflows like onboarding and off-boarding, along with the current password reset procedures changing. There is also a technological aspect impacted, as there will need to be confirmation that any legacy systems are compatible with the new approach of MFA and there will also be updates to any logging and monitoring taking place. Systems thinking helps to prevent unintended consequences as a result of changes to processes, infrastructure or mitigation tactics and analyzing dependencies ensures a balanced view of potential impacts to support sustainable implementation while avoiding operational disruptions and downtime.

Evaluating Evidence to Determine Decision Quality:

Risk-informed decisions must demonstrate measurable improvement with evidence, and that evidence can be in the form of lowered risk ratings within Risk Registers after controls are implemented, fewer actual security incidents and/or faster detection and response metrics, audit compliance as a result of adhering to the frameworks outlined like NIST and CIS, and operational continuity measurements which confirm that an organization's systems are resilient and avoiding disruptions. When determining if a good decision was made regarding a risk and the mitigation tactics surrounding it, the mentioned quantifiable metrics are all useful and are able to be verified, while qualitative data could also be useful such as feedback from employees/users and their experiences in using the systems on a daily basis. For example, if an organization were to implement network segmentation paired with strict monitoring, there should be a measurable reduction of unauthorized access and no disruptions experienced by authorized users, which confirms that the risk-informed recommendation was valid and achieved its intended goal without causing other issues.

Risk-informed recommendations are vital for organizations to uphold resilience and security, and they must be based on structured approaches, reliable tools, authoritative resources, and objective data-driven evidence. Using tools such as Risk Registers, BIAs, SIEMs, vulnerability management platforms, and systems thinking enables Analysts and organizations to quantify risks and justify recommendations with actual evidence. Following industry-standard frameworks like CIS and NIST CSF enable defendable basis of prioritization, with biases being minimized through standardized scoring and peer validation while systems thinking ensures recommendations always consider impacts on a holistic level. Evaluating decisions with measurable evidence in the form of improved metrics confirms whether recommendations are

achieving their intended outcomes of systems and data security, which in a time of sophisticated threats and breaches is crucial. Organizations that utilize data to create risk-mitigation strategies have a distinct competitive advantage to others who don't utilize a structured approach in their decision-making.

References

Peacock, J., (n.d.). *Risk Register Examples for Cybersecurity Leaders.* CyberSaint Security. Retrieved on December 11, 2025 from: https://www.cybersaint.io/blog/risk-register-examples-for-cybersecurity

National Institute of Standards and Technology, (June 27, 2024). *National Vulnerability Database: Vulnerability Metrics.* NIST. Retrieved on December 11, 2025 from: https://nvd.nist.gov/vuln-metrics/cvss

Swanson, M., et al., (May 2010). *Contingency Planning Guide for Federal Information Systems. SP 800-34 Rev. 1. Chapter 3.2.1.* National Institute of Standards and Technology. Retrieved on December 11, 2025 from: *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*

Geeks for Geeks, (July 23, 2025). *OpenVAS: Security Assessment.* Geeks for Geeks. Retrieved on December 11, 2025 from: https://www.geeksforgeeks.org/computer-networks/security-assessment-openvas/

Framework Security, (May 2, 2025). *The Target Breach: A Historic Cyberattack with Lasting Consequences.* Framework Security. Retrieved on December 11, 2025 from:

https://frameworksecurity.com/post/the-target-breach-a-historic-cyberattack-with-lasting-consequences

NIST, (February 26, 2024). *The NIST Cybersecurity Framework (CSF) 2.0.* National Institute of Standards and Technology.

Retrieved on December 11, 2025 from:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

CIS, (n.d.). *CIS Critical Security Controls.* Center for Internet Security.

Retrieved on December 11, 2025 from:

https://www.cisecurity.org/controls

CIS, (n.d.). *The 18 CIS Critical Security Controls.* Center for Internet Security.

Retrieved on December 11, 2025 from:

https://www.cisecurity.org/controls/cis-controls-list

Wit, J., & Meyer, C., (May 1, 2022). *Uncovering Cognitive Biases in Security Decision Making.* Security Management.

Retrieved on December 11, 2025 from:

https://www.asisonline.org/security-management-magazine/articles/2022/05/uncovering-cognitive-biases-in-security-decision-making/

Scrut Automation, (April 17, 2025). *Mastering Quantitative Risk Assessment and Analysis: A step-by-step guide in 2025.* Scrut Automation. Retrieved on December 11, 2025 from: https://www.scrut.io/post/mastering-quantitative-risk-assessment-a-step-by-step-guide