DEPARTMENT: CYBERSECURITY

What’s Your IT Risk Approach?

Linda Wilbanks
US Department of Education

Editors:
Rick Kuhn, NIST;
d.kuhn@nist.gov

Tim Weil, Alcohol
Monitoring Systems;
tweil.ieee@gmail.com

Risk is the likelihood that a loss will occur. Losses occur when a threat exposes vulnerability. To identify risks, you need to identify the threats and vulnerabilities and then estimate the likelihood of a threat-exploiting vulnerability. Risk management starts with an understanding of the threats and vulnerabilities, after which the appropriate mitigation action is identified. It is a series of coordinated activities to direct and control challenges or threats to achieving an organization’s goals. Enterprise Risk Management (ERM) is an organization-wide approach to addressing the full spectrum of the organization’s significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos.

Cybersecurity risk is the risk to an organizational operation’s mission, function, image, reputation, organizational assets, individuals, and the nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. Information system–related security risks are those that arise through the loss of confidentiality, integrity, or availability of information systems. Cyber risk, like any other type of risk, cannot be eliminated—it must be managed. Effective cybersecurity demands the shared responsibility of all. The management of organizational risk is a key element of an enterprise-wide information security program that provides an effective framework for minimizing risks from security threat.

The objective of a cybersecurity risk-management program is to provide an integrated view of IT risk across the entire organization and to ensure that risk issues are integrated into the strategic decision-making process to further the achievement of performance goals. Within the US Department of Education’s Federal Student Aid (FSA) cybersecurity risk-management program, the objective is to strengthen information technology systems’ security through effective risk management, understand the threats and vulnerabilities, and then mitigate the risks or reduce the potential impacts. Effectively managing cybersecurity risk is a continuous activity and requires communication across all levels of an organization.

OMB Circular A-123’s *Management’s Responsibility for Enterprise Risk Management and Internal Control*[1] requires all federal agencies to implement an ERM capability. ERM is the discipline that identifies, assesses, and manages risks to all concentration of efforts toward key points of failure and reduces or eliminates potential disruptive events. ERM is part of the overall governance process and is an integral part of cybersecurity risk management, ensuring that actions taken support the enterprise mission and goals. It provides a holistic approach to managing risk opportunistically to achieve maximum results for the enterprise.

2469-7087/19 © 2019 IEEE

CYBER RISK MANAGEMENT FRAMEWORK (CRMF)

NIST Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*,[2] shifts the focus away from a certification and accreditation compliance approach toward continually assessing risk and security authorization—a more active monitoring of the system through its system development lifecycle.

The Cyber Risk Management Framework (CRMF) builds flexibility into the overall information security lifecycle to address the increasing nature and scope of threats in real time, providing a number of key advantages that include the following:

- continually evaluating the organization's risk posture and maintaining situational awareness of its cybersecurity posture;
- understanding the state and maturity of an agency's cybersecurity program;
- evaluating cybersecurity programs at key vulnerability points: people, processes, and technology;
- maintaining a focus on the security program lifecycle; and
- addressing the key functions (governance, risk, management, compliance, operations) of a security program.

The CRMF emphasizes three main principles:

- integrating information security into the system development lifecycle and applying best practices for secure development and engineering up front and throughout the lifecycle of an information system;
- monitoring and maintaining ongoing situational awareness of information system status through both manual and automated means, and continuously improving upon reporting processes to achieve greater situational awareness; and
- making informed risk decisions (and accepting risk) based on a complete understanding of the impact to operations and assets, individuals, other organizations, and the nation.

To establish a robust CRMF that is supportive of an organization's mission, the CRMF must utilize the ERM and be integrated into the business processes. Cybersecurity risk management cannot be effective in a silo.

Organizationally, the CRMF is designed to support the management of cybersecurity risk at multiple organization levels. The intent is not to escalate or elevate all cybersecurity risk decisions to the most senior levels, but to establish clear boundaries and business processes to enable the flow of risk information for decisions to be made at the appropriate levels. Establishment of thresholds for decision making that are based on organizational risk associated with system weaknesses and vulnerabilities is essential for effective CRMF operation.

To ensure that critical risk information is reaching the appropriate organizational stakeholders responsible for the development of policy, planning, and execution of cybersecurity resources and assets, the organization must implement a strong but agile governance and oversight model utilizing ERM. The CRMF governance and oversight model supports the flow of information between organizational levels, promotes transparency in decisions, and provides the mechanisms necessary for information assurance and security to be fully integrated into the business processes such that it is a true enabler of the mission and is not perceived as an inhibitor to progress.

> Cybersecurity risk management cannot be effective in a silo.

The 2017 Presidential Executive Order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"[3] requires federal agencies to utilize the CRMF and to explicitly document cybersecurity risk mitigation and acceptance choices, including any decisions to not mitigate known vulnerabilities in a timely manner.

CYBERSECURITY RISK INDICATOR (CSRI)

The US Department of Education's FSA has an ERM program that provides strategic direction for assessing, monitoring, and managing risk and includes strategies for managing risk that conform to the risk profile and risk appetite; capabilities and methods for identifying, assessing, quantifying, and managing risks; and formalized methodologies for risk assessments at all levels within FSA. Cybersecurity risk management presents unique challenges in evaluating and determining risks. FSA has more than 90 systems in its inventory—some are Federal Information Security Management Act (FISMA)–reportable and some are classified as mission critical by federal guidelines. However, these are isolated pieces of information about the systems; there is no clear methodology for comprehensively determining a system's cybersecurity risk.

FSA determined that a quantifiable methodology was needed to measure system cybersecurity risk. The concern was that without a quantifiable methodology to evaluate cybersecurity risks,

- systems identified as highest risk could be based on knowledge of the system and/or experience with it and unknown systems might not be considered high risk,
- system cybersecurity risk might not be considered during resource evaluations, and
- systems that have higher cybersecurity risks might not be properly protected or receive the necessary resources.

In response, I developed the Cybersecurity System Risk Indicator (CSRI), a cybersecurity evaluation methodology that is utilized within FSA and the US Department of Education to assist in resource allocations and identify systems that might pose a higher risk to vulnerabilities or threats. The CRSI focuses only on the risks posed by aspects of information technology.

For each FSA system, the CSRI utilizes 26 risk factors that can indicate whether a system is a higher risk using federal indicators (such as FISMA reportable), IT architecture (such as interconnections, cloud-based, personally identifiable information), FSA-specific risk factors (such as physical location of the system and external partners), and known system vulnerabilities and accepted risks.

Each of the 26 factors is weighed because not all factors indicate the same level of risk. A scale of 1 to 4 is used—higher weight indicates higher risk. The factors and weights are shown in Table 1. These were developed for FSA systems—each company will need to identify the appropriate factors and weights based on their organization's level of acceptable risk.

For each factor, the possible responses were identified (shown in parentheses) and assigned a value between 1 and 5 (5 indicating the higher risk response). As this is a new process and is still being modified and the system inventory is being updated, many factors were rated yes/no until further information is entered into the inventory.

Table 1. Risk factor per system.

DHS high-value asset (yes/no)	4
Authority to operate status (3 years or ongoing)	3
Classification system type (major, minor, GSS)	3
Cloud-based system (yes/no)	3
Criticality rating (mission critical)	3
External partner security management (yes/no)	3
FIPS-199 rating (major, minor)	3
FISMA reportable (yes/no)	3

Interconnections (yes--number/no)	3
Past-due plan of actions and milestones (POAMs) (count, criticality, aging)	3
Accepted risks (count, criticality, aging)	3
Personally identifiable information (yes/no)	3
System outside of FSA (external partner site) (yes/no)	3
Date of last audit (1 years, 2 years…)	2
E-authentication utilized (yes/no)	2
Non-POAMs (count, criticality)	2
Number of users (count)	2
Servers public facing or in DMZ	2
Sub-systems/minor applications within system boundary (yes--count/no)	2
Systems PIV-enabled (yes/no)	2
User base (internal, external)	2
Web-based system (yes/no)	2
Continuous monitoring (yes/no)	1
COTS-based (yes/no)	1
MOU expiration date (1 year, 2 years…)	1
Recovery time objective (hours)	1

The CSRI for each system is calculated as follows.

a.) Utilizing the data for the factors using the FSA system inventory, score each of the 26 factors.
b.) Multiply each score by the weight for that factor.
c.) Results of b.) are summed for the system's CSRI result.

The result is a list of scores for each system (see Table 2).

Table 2. Sample Cybersecurity Risk Indicator (CSRI) results.

System	CSRI score
A	237
B	190
C	168
D	111
E	67

The scores alone have no value at all; the value of the CSRI is in the comparison of the scores when determining, based on cybersecurity risk, where resources should be allocated to best protect the company's assets. Applying the methodology also helps identify the specific cybersecurity risks to each system.

The methodology was reviewed by IT and cybersecurity subject matter experts within FSA and the US Department of Education. Changes were made and the final methodology has been utilized for three quarters and continues to be revised to clearly articulate the cybersecurity risks.

CONCLUSION

Risk management is the recognition that you cannot protect against everything—it is about prioritization and the acceptance of risk. Governance is important and a framework is critical. IT systems are the heart of any company. Advance planning and risk management are the keys to appropriately protecting your networks, systems, and data—your company's critical assets.

REFERENCES

1. *Management's Responsibility for Enterprise Risk Management and Internal Control*, executive order, Office of Management and Budget, Executive Office of the President, 15 July 2016; www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.
2. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, government report Special Publication 800-37, Revision 1, NIST, 2010; https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf.
3. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, executive order 13800, 11 May 2017; www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure.

ABOUT THE AUTHOR

Linda Wilbanks is the Senior Cyber Risk Advisor at Federal Student Aid (FSA) in the US Department of Education. She is also the Associate Editor of Columns and Departments for *IT Professional*. Contact her at linda.wilbanks@ed.gov.

This article originally appeared in
IT Professional, *vol. 20, no. 4, 2018.*