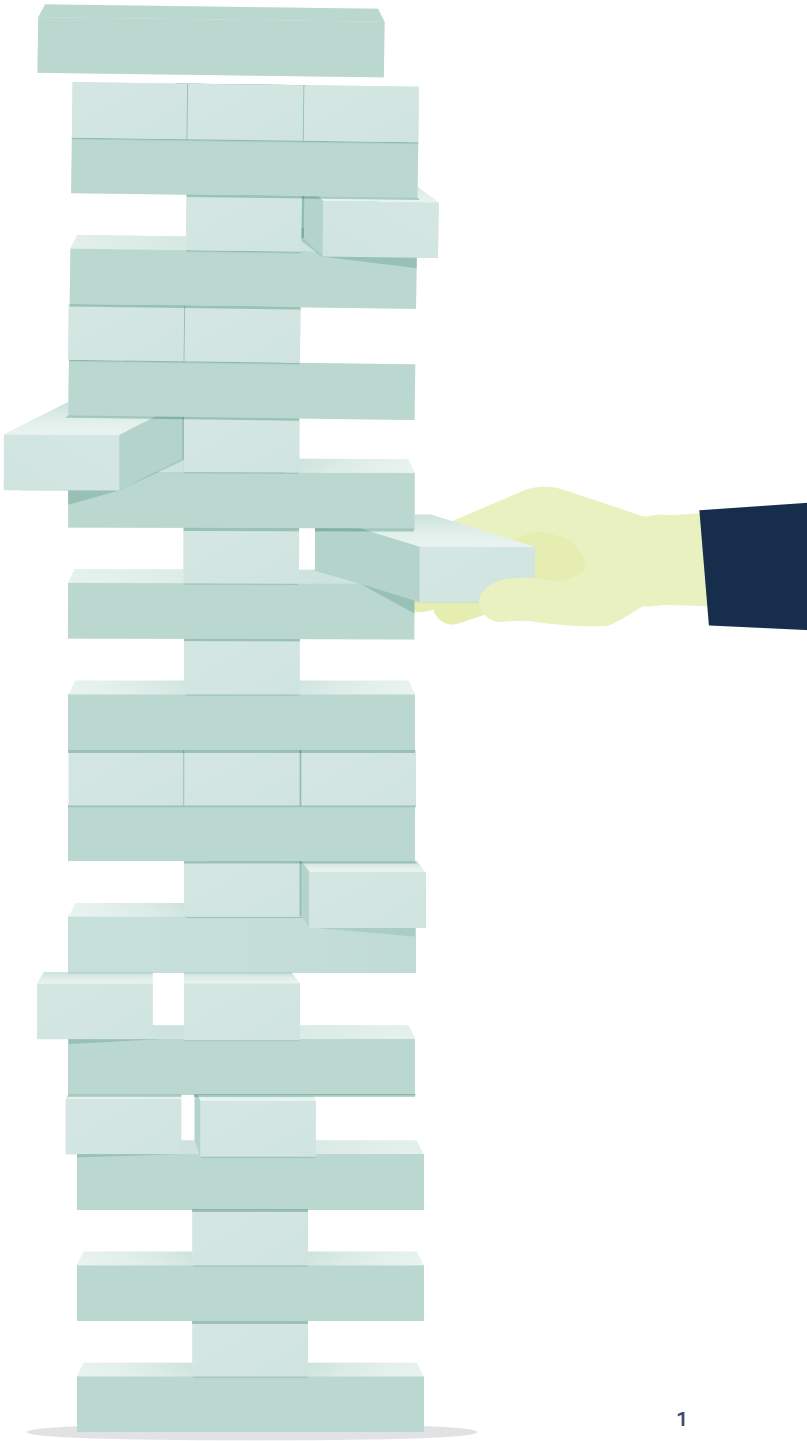
Enterprise Risk Management in Today's Digital World



GOVLOOP
E-BOOK
2019

RSA carahsoft govloop

Executive Summary

As the government's reliance on digital technologies expands, it's becoming increasingly challenging to secure the growing network of devices, IT systems and cloud solutions. What makes today's digital environment so unique is that security extends beyond the perimeter of government offices.

The traditional check-the-box approach to security that agencies use to comply with Office of Management and Budget (OMB) requirements and cybersecurity practices in the Federal Information Security Management Act isn't sustainable. Instead, they must assess what they own and manage, how critical those assets are to government operations, how best to secure them and what levels of risk are acceptable versus what needs mitigation.

The reality is that IT risks cannot be completely eliminated, especially in this digital era; they must be managed. "[But] for the better part of the past decade, OMB, the Government Accountability Office (GAO), and agency inspectors general have found that agencies' enterprise risk management programs do not effectively identify, assess, and prioritize actions to mitigate cybersecurity risks," according to the Federal Cybersecurity Risk Determination Report and Action Plan, released in May 2018.

That's not for a lack of interest or trying. OMB issued Circular No. A-123 in 1981 "to improve accountability in Federal programs and operations," and updated it in July 2016 to reflect the burgeoning digital environment. The National Institute of Standards and Technology (NIST) built on that by issuing The Risk Management Framework in December 2018 that prepares "organizations to execute the framework at appropriate risk management levels."

Risk management is top of mind at the state and local government levels, too. It has topped the National Association of State Chief Information Officers' (CIOs) annual top 10 list of priorities for six years running.

In "Enterprise Risk Management in Today's Digital World," we explain what an enterprise approach to risk management looks like in government today and why it's necessary to support government's digital future.

The History of Risk Management in Government

The need for risk management in government has grown along with agencies' digital footprints. That's because the more complex the environment, the more vulnerable it becomes. Here's a look at where governments at all levels stand with risk management.

74%

of the 96 agencies participating in the risk assessment process have cybersecurity programs that are either at risk or high risk.

49%

of agencies can detect and whitelist software running on their systems.

17

agencies out of 23 that the GAO studied have not fully established agency- and system-level policies for assessing, responding to and monitoring risk.

42%

of local government IT officials say their agencies have adopted a cybersecurity framework based on national standards and guidelines.

13 of 15

program risks at the Internal Revenue Service lacked detailed descriptions of risk mitigation plans, and 12 lacked detailed descriptions of mitigation activities.

4%

of 204 local governments in the United States show some aspect of enterprise risk management (ERM).

2 of 5

chief information security officers said they were reviewing NIST's Cybersecurity Framework on release.

80%

of the problem with risk management is cyber hygiene, the Chief Information Security Officer for the Air Force's Office of the Deputy CIO said.

"There is an urgent need to further strengthen the underlying information systems, component products, and services that we depend on in every sector of the critical infrastructure — ensuring that the systems, products, and services are sufficiently trustworthy throughout the system development life cycle (SDLC) and can provide the necessary resilience to support the economic and national security interests of the United States."

Risk Management Framework for Information Systems and Organizations

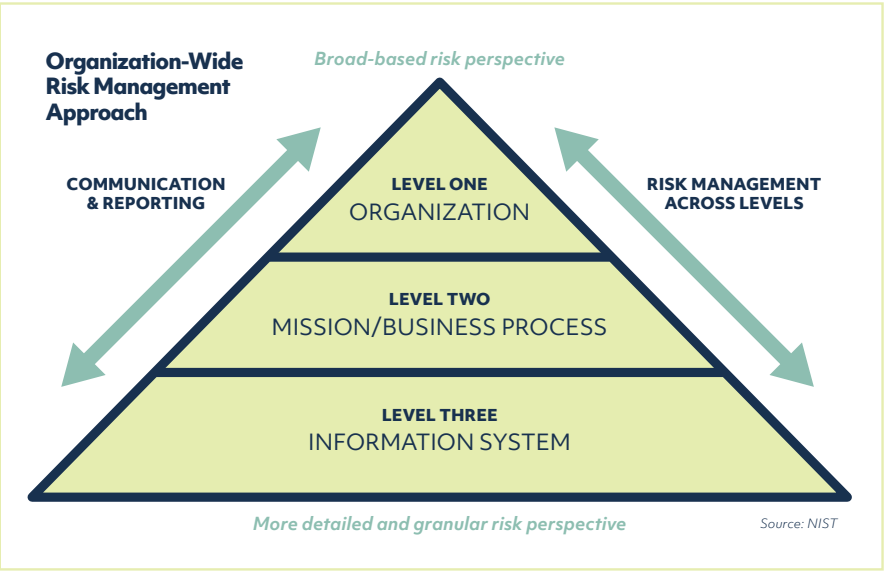
69%

of state cybersecurity budgets went to compliance and risk management in 2016, down from 74% in 2014.

Digital Risk Management at a Glance

Evolution of ERM

It used to be that government agencies' IT fit almost in a literal box — all computing took place within the confines of the building. As a result, containing risks was relatively simple: Slap a firewall around the network, teach employees not to click questionable links and continue with business as usual.



But the technological revolution of the past few decades has landed agencies in a precarious position. On one hand, new and more powerful computing power lets governments be more productive. Mobile, cloud and edge computing have revolutionized governments' IT environments, making it easier for agencies to meet their missions and citizens' demands.

What's more, technology has become not only ubiquitous, but the public and private sectors have become dependent on it, which is why it's unfortunate that the flip side of these benefits is significantly increased vulnerability.

That's because as agencies replace existing infrastructures with modern ones or fold in emerging technologies to their legacy systems, they expand their attack surfaces, giving hackers and malicious insiders more ways in. IT officials must weigh the pros and cons of each new technology to determine whether it's worth the damage that could be wrought should hackers successfully exploit those vulnerabilities.

"The significant increase in the complexity of the hardware, software, firmware, and systems within the public and private sectors (including the U.S. critical infrastructure) represents a significant increase in attack surface that can be exploited by adversaries," according to NIST's Risk Management Framework for Information Systems and Organizations.

What exactly is risk management? It's **"a coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives,"** according to a playbook from the Chief Financial Officers (CFO) Council and Performance Improvement Council. By contrast, ERM "is an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos," it states.

4 Steps to Effective ERM

Aspects of agencies' ERM needs are unique, but there are four steps that apply in every case.

1. Frame how you'll manage risk.

This involves studying all the risks — financial, reputational, programmatic, cyber and privacy, for example — that feed into the ERM equation. Determine what risks you actually face and which could arise in the future.

2. Inventory your environment.

Understand what makes up your IT infrastructure, what devices employees use to connect to the network, what software is running and all other components that make up the system. Then break it down further to determine how critical each piece of technology is to the mission and what vulnerabilities may lurk within them, such as the hardware, software and firmware that make up the system.

3. Mitigate the risk.

What risk are you willing to accept, and what requires a response? One approach is called whitelisting, which means you allow only certain applications to run on your system. It helps guarantee that only those applications that you've deemed trustworthy can execute on that computing machine.

4. Monitor for new risks.

IT environments are fluid, with technology, software and users going in and out at a dizzying pace. Agencies must assess how each change affects that baseline security posture.

Challenge: The Supply Chain

One area where governments are struggling to manage risks is in the supply chain. They may have done due diligence in researching a vendor from which they're buying a new system, but did they also study the components of that system to understand where they were manufactured or what the reputation of those companies are? For instance, on Sept. 10, 2019, the federal government banned agencies from using any products from Russia-based Kaspersky Lab after concerns surfaced about its executives' ties to Russian government officials.

Increased reliance on contractors and commercial solutions means attacks or disruptions in the supply chain are also increasing in the form of tampering, such as inserting counterfeit parts or malicious software; theft; and a lack of built-in security capabilities. Supply-chain risk management, therefore, is a natural partner to ERM.

OMB Circular A-130 requires third-party providers handling government information or operating systems on behalf of agencies to meet the same security and privacy requirements as those agencies, and companies can use RMF to reduce supply-chain risks. Still, as much as 80% of security breaches occur through the supply chain.

ERM Success Story

Public or commercial cloud is one example of the give and take that ERM involves — and how the scales can be tipped in government's favor. The upside to cloud computing is that it makes agencies more effective and efficient, opening them to capabilities such as big data analytics, the Internet of Things and artificial intelligence-driven initiatives. What's more, cloud can shrink physical footprints by moving applications and data offsite, out of environmentally unfriendly, budget-busting data centers.

But there are downsides, too. For instance, cloud service providers, which own and operate the cloud, could have different security standards. For a long time, that was such a deterrent that security concerns kept agencies from adopting cloud despite all the benefits. The Federal Risk and Authorization Management Program (FedRAMP) has changed that.

Established in 2011, FedRAMP evaluates cloud products and services against rigorous standards, going far in reducing those concerns. Forty more agencies began participating in the program in 2018, and the number of FedRAMP-authorized products jumped 60 percent between 2017 and 2018. An April 2019 GAO report found that agencies have increased cloud usage.

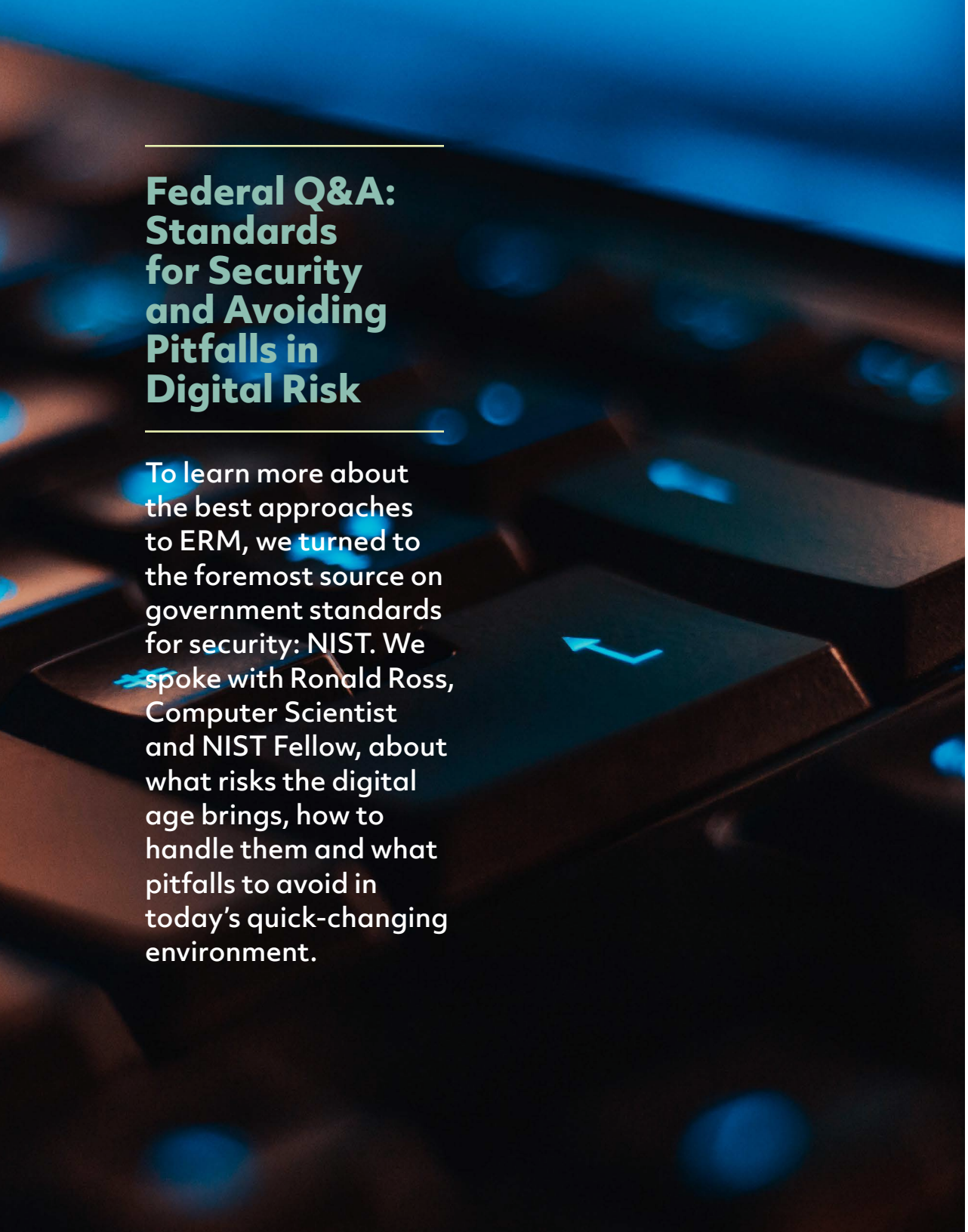
Government's Helping Hand

ERM is getting a boost from other federal initiatives. For instance, NIST's Risk Management Framework (RMF) for Information Systems and Organizations updates previous guidelines to connect the NIST Cybersecurity Framework to RMF, institutionalize critical risk management preparations and integrate privacy risk assessments into RMF.

Despite these efforts, "agencies do not understand and do not have the resources to combat the current threat environment," according to the Federal Cybersecurity Risk Determination Report and Action Plan. Thirty-eight percent of federal cyber incidents had no identified attack vector, for instance.

IT officials and agency leaders must work together to consider all risk sources, what they mean for operations, how they can best be mitigated and how the agency could be affected if hackers successfully exploit them. Then, they need to assess whether all that is worth it, both in terms of a dollar figure and reputation loss. As seen with the Office of Personnel Management data breach — which is estimated to have cost between $133 million and $1 billion — digital incidents can be costly.

To securely and efficiently operate in today's digital environment, agencies need robust security practices that enable seamless government services. They require greater collaboration between the teams that focus on risk management, security and business operations. To make this a reality, agencies need a unified approach to managing digital risks.



Federal Q&A: Standards for Security and Avoiding Pitfalls in Digital Risk

To learn more about the best approaches to ERM, we turned to the foremost source on government standards for security: NIST. We spoke with Ronald Ross, Computer Scientist and NIST Fellow, about what risks the digital age brings, how to handle them and what pitfalls to avoid in today's quick-changing environment.

GovLoop: What risks do federal agencies face in an increasingly digital environment?

With regard to digital technology, the risk assessment focuses on what components do I have in my system, what kind of software am I running, what's my mission, how critical is the technology to the mission — the vulnerabilities that may exist in those software products and in the hardware and the firmware, all the parts that come together as part of that system. You have to assess the risk that is there based on the type of technology you're using and how you're using it. After you assess the risks that you have, then you look toward responding to the risk. Sometimes organizations will accept the risk, and sometimes they're not going to accept it and they're going to do some additional response actions, or mitigations, to close down certain vulnerabilities.

In the risk assessment business, we're looking at threats and the vulnerabilities and then mission or business impact if the threat actually exploits a particular vulnerability you have in your system. There's a likelihood component to that. In the digital world, the likelihood is close to 100%. Our adversaries out there are very sophisticated. They understand the vulnerabilities in our systems, they understand who they're targeting, and so there's a pretty good likelihood either you have been attacked or you will be attacked

soon. That's the kind of climate we're working with in the digital world — total dependence on technology, a highly vulnerable infrastructure of IT components — and we have to do the best we can to close down those vulnerabilities as quick as we can and, moreover, try to minimize the damage if the adversaries carry out a successful attack.

How did we get here?

We've just built an incredibly complex system and system of systems. We're building a fully digital world, and in that complexity, if you don't spend some time figuring out how all those things work, how they're put together, where the information flows, where are my vulnerabilities, that complexity is where the adversaries live every day. They know it's complicated, they know we can't keep track of it all and therefore they always have the advantage.

How can agencies address these risks?

Figure out what your critical assets are and implement stronger protective measures for those places in your system. This is really a two-part problem. People who run enterprises can't build software and all the security features that are necessary to protect the systems, just like Honda doesn't ask me to go out and get my own airbag and put it in the car. [There are] certain responsibilities that industry has to step up and face: How are they going to build better security features into the products and systems that every customer is using today, from smartphones to power plants to medical devices? The other half of that point is then what the consumers, who are in federal agencies and private sector organizations, can do to help reduce the risk. We try to start with a critical asset analysis and then we try to encourage them to reduce their digital footprint, or attack surface. So, we encourage agencies to minimize the functions and features on the system, minimize the number of components that are mission-essential, especially when you're supporting critical missions, critical programs and critical assets.

What are some best practices that agencies can look to?

The RMF that we have helps organizations identify which controls do I actually need, which ones can I get by without and what are my residual risks if I select these particular controls and implement those correctly? Then they can communicate back up the chain to the C-suite about how this organization really looks now in the real world of operations after they've done everything they can do to stop the bad guys. The best practices are reflected in the Cybersecurity Framework, they're reflected in the Risk Management Framework, they're reflected in our security controls and privacy controls document.

What should agencies look to for the future?

If we're going to succeed and actually manage risk and carry out critical missions, we're going to have to conquer and get our arms around this complexity issue. When you go through and identify your critical assets, you can then move those to safer locations; you can build security domains for those critical assets that will allow you to protect those assets to a much higher degree. We have our federal cloud computing controls that industry has adopted, and so when you get to the mid-level information that's not your most critical stuff, you can start to think of moving some of that to the cloud to take advantage of more efficient ways of computing, providing better services to your customers, and then you thin that environment that exists within the federal agency. The cloud providers are deploying some of the best people on the planet who understand security and they're protecting that cloud operation. Then you can focus on the critical assets back home. **If you try to manage your risk across all of your efforts and all that complexity, you will fail.** You have to get some help, and you have to organize for battle.

Calibrating Your Digital Risk in a Rapidly Evolving World

An interview with Robert Carey, Vice President and General Manager of Global Public Sector Solutions, and Dan Carayiannis, Public Sector Director, RSA Security

Today, the need for risk management in government has grown along with agencies' digital footprints. That's because the more complex the environment, the more vulnerable it may become.

To securely and efficiently operate in today's digital environment, agencies need robust security tools and practices that enable seamless government services. They need greater collaboration between the teams that focus on risk management, security and how the network supports critical business operations.

To make this a reality, agencies need a unified approach to managing digital risks. To learn more about digital risk management, GovLoop sat down with Robert Carey, Vice President and General Manager of Global Public Sector Solutions, and Dan Carayiannis, Public Sector Director at RSA Security. RSA provides mission-critical cybersecurity capabilities for government agencies worldwide.

"Digital risk management is really the understanding of the mission or the business as it maps to the network, and the technologies that are within the network," Carey explained. **"It's understanding the exposure of risk as organizations embrace new technologies, whether it's mobile, cloud computing, AI or more."**

The need for digital risk management has accelerated as government expands its IT infrastructures and technology footprints, Carayiannis added.

"This concept of moving from more of a traditional IT infrastructure, to one where they're embracing more of the new digital technologies, the shift to new technologies can oftentimes present unexpected risks," Carayiannis said. "For agencies that are trying to leverage new technologies and capabilities, but not really thinking about the possible downstream risks that they might bring upon themselves, they could be opening themselves to a plethora of negative consequences."

An added dimension of risk that government organizations need to consider and address is third-party risk. Departments and agencies are increasingly leveraging third parties to support mission and business operations. In many cases these organizations provide added capabilities and expertise often times at a reduced cost. At the same time, government organizations need to respect the fact that these third and even fourth party organizations are now part of their "extended risk ecosystem" and as such need to be managed, controlled and inspected accordingly.

So what can agencies do? RSA Archer Suite is one solution that empowers organizations of all sizes to manage multiple dimensions of risk on one configurable, integrated software platform.

With RSA Archer, organizations can quickly implement risk management processes based on industry standards and best practices — leading to improved risk management maturity, more informed decision-making and enhanced business performance.

"Archer provides visibility or command and control of what's going on in the network," Carey said. **"That allows agencies to manage what's going on in detail to the network, still leverage new technologies to meet mission, and keep their infrastructures safe as they move into the future."**

Takeaway: Government has long derived value from the network and their IT to accelerate their mission outcomes. In today's complex world as technologies evolve very quickly, and they are embraced and embedded in the network to derive that value, calibrating your digital risk is critical.

What is Digital Risk?

Digital risk refers to the new and often unexpected consequences of digital transformation, and it's becoming a top concern for business and IT executives.

Explore RSA's growing library of research, webinars, videos, and more at https://carah.io/RSA-Digital-Risk

A Definitive Guide to Managing Digital Risk

RSA®

State & Local Q&A: Creating Scorecards to Better Communicate Risk

The IT and security teams aren't alone in managing risk at organizations, but they are often the ones who understand it best. To help other government officials understand risk and their role in minimizing it, Minnesota IT Services (MNIT) created Risk Management Scorecards that have fostered communication — and security — since 2015. We spoke with Aaron Call, Chief Information Security Officer at MNIT, to learn more.

GovLoop: How have risks evolved in your state along with the growth of digital?

Risks have evolved for the state very similar to the way the risk has evolved for anybody in the private sector as well. Well-funded adversaries continue to use the expanded footprint of IT against us. What's unique in the public sector is that we're also prime targets for politically motivated attackers to a degree that most private sector organizations aren't.

In 2015, you created the Minnesota IT Services Risk Management Scorecards to address those risks. What are the advantages of having them?

We recognized that we can't meet this evolving threat as a security silo. A security program of any organization can't do this alone, and we have to have investment — not necessarily just in money, but also in priority — with the business leaders. You can play Chicken Little. You can tell them how scary the world is and try to compel them that way, or you can go down a more respectful path and present that risk that they own ultimately through their own business decisions, help them understand how those business decisions impact risk.

In 2015, we gathered together a number of metrics that we iterate on every couple of years. We roll each of those metrics up

into a weighting for particular relevance into five different areas based on the NIST Cybersecurity Framework functional areas. So, what we're telling them is not how effective their antivirus is or how well-patched their systems are. What we're telling them is how well we can identify the systems and data that support their business, how well are we able to prevent attacks from happening and how well we can detect attacks, whether they're successful or not. When a cybersecurity event does occur, [we show] how effective we are at stopping it from spreading or [stopping] it from happening again, and whether it's "Here's a related incident" or just some bad luck, [we show] how well we are equipped to bring the IT systems that support their services back online. Those five areas — identify, protect, detect, respond and recover — are easily understood, they're non-geeky and they give us an opportunity to then describe to the business leaders, "This is what this needs."

Do you have a scorecard success story?

We've got some tactical wins where conversations around the risk scorecard highlighted something that surprised a business leader or brought light to risk that they weren't comfortable accepting, and they were able to address that. In the broader sense, it's also created more of an atmosphere of trust between the business leaders and the security teams. Today, more than any time in the past and hopefully continuing forward, when security suggests something or tries to drive an additional control or a change in a technology, the resistance is really quite minimal in most cases.

How are you preparing for future risks?

Despite being a security leader, I see security as being a silo, as being horribly inefficient and that's something that needs to be as much as possible eliminated. The fact that I have tax dollar-paid staff within the state doing just security work, they're not directly providing value or services to our citizens, so if we can accomplish the same security by having IT and business staff behave in more secure ways or equip them with more secure tools, then we can eliminate that cost. That's a leading philosophy for how we move forward: Where can we make things secure by default, and where can we make things secure out of the box so we don't have to do that ineffective and inefficient security bolt-on?

What are a few lessons learned?

The best lesson learned is the importance of having the right people communicating those scorecards to the business. What we put together wasn't particularly novel. The real value, though, is making sure that a respectful and informed conversation is happening. Most security people can use the scorecard. They can determine what an agency's relative risk is in each of these areas. But not everybody can sit down with a commissioner or a deputy commissioner and talk to them about their risk. Many times simply by presenting them with this information, they have to own it. That's not a position every commissioner, deputy commissioner, political animal really wants to be in, so being respectful of that yet getting the information across to them really is a soft skill that not everybody has. The departments and agencies that we've been more successful at with the risk scorecards tend to be those where we had security leaders that had those skills.

Conclusion & Next Steps

The truth is that risk is unavoidable in carrying out an organization's objectives, but it can and must be managed. Modern technology can take government agencies to the next level of capabilities, services and mission attainment, but an oversight could undo all that progress in a heartbeat.

By following guidelines to build an enterprisewide foundation for ERM and implementing a practice of continuous monitoring afterward, agencies at all levels of government can strengthen their security posture, make the most of emerging technologies and increase public trust in their ability to protect not only their personal data, but the nation's critical assets, too.

Here are six steps to follow when putting together an ERM model based on the CFO playbook:

- **Establish Context:** Consider policy concerns, mission needs, stakeholder interests, agency culture and the level of risk the agency is willing to accept for specific technologies, programs and the agency as a whole.
- **Identify and Categorize Risks:** Ask what could happen and how program areas or objectives would be impacted. Then, take a page from the Cyber Threat Framework and create a color-coded mitigation coverage map. Green means there is at least one capability that mitigates the threat at the "significant" level, yellow signifies that at least one capability mitigates a threat at a "moderate" level, pink means at least one capability mitigates a threat at a "limited" level and red means no capabilities exist to mitigate the threat.
- **Analyze and Evaluate:** Consider the root causes and sources of the risks you've identified, and estimate the probability that they will occur — and the potential positive and negatives outcomes that could result.
- **Develop Alternatives:** Find ways to accept, transfer, share, avoid or mitigate major risks and compare the cost of mitigation with that of exposure. This includes non-financial costs, such as irreparable reputational damage.
- **Respond to Risks:** For risks you want to address, allocate resources such as budget and savvy employees who can help. Document milestones for carrying out the risk management process.
- **Monitor and Review:** At a minimum, schedule the review semiannually, but note that even small changes can have a big impact on critical technology.

Additional Resources on ERM

- Improving Government Decision Making through ERM
- Federal Information Security Modernization Act of 2014
- Supply Chain Risks Affecting Federal Agencies
- The Agency HVA Process
- How Local Leaders Can Ensure a Safe and Secure Cyber Environment
- Making the Grade: Improving Risk Management on the FITARA Scorecard 8.0

Thank you to RSA and Carahsoft for their support of this valuable resource for public sector professionals.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop