Opportunities to protect the enterprise leveraging NIST 800-53 Revision 5

As the world continues to become more digitized and connected, the risks themselves are also changing, which opens systems and data to potential cybersecurity attacks. For the first time since 2013, the National Institute of Standards and Technology (NIST) has published the special publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations — which aims to assist public and private organizations better manage their risk — focusing on a "new state-of-the-practice controls." Following the guidelines is voluntary in the private sector; however, NIST encourages the private sector to adopt the new guidelines, just as many have already adopted NIST's Cybersecurity Framework (CSF).

NIST's update and expansion to its flagship catalogue of controls creates an opportunity for those protecting the enterprise to leverage the "next generation of security and privacy controls" by going beyond compliance, integrating privacy and security efforts, and addressing complex supply chain risk management.

Beyond compliance

Ernst & Young LLP (EY) supports public and private organizations by providing consulting and audit services. Through these efforts, we have developed a mature framework and methodology for optimizing the effectiveness of information security controls. In providing these services to our clients, we have observed that many face similar challenges and are allocating significant resources in responding to a growing and more complex regulatory environment. **This has resulted in the accumulation of layers of redundant, ineffective and misaligned controls, which is costly to the organization, inefficient and rarely addresses risks sufficiently.** It has also resulted in the inability for the entities to holistically apply existing controls to address multiple risks and objectives simultaneously, including cyber-security and business operations. Rather than mapping controls to objectives and risks enterprise-wide, organizations are performing duplicative testing at significant cost and time to the organization.

With the effort of making NIST 800-53 Revision 5 controls "outcome-based" — organizations should develop and implement an integrated and effective testing strategy that allows for the NIST 800-53 Revision 5 testing results to be leveraged across different regulatory frameworks that are supported by quality-based evidence that go beyond the traditional paperwork exercise. In our experience, agencies spend millions of dollars in their NIST 800-53 assessment efforts; however, these efforts often fall very short against other independent assessments, can't be leveraged beyond the authorization to operate (ATO) compliance exercise and, most importantly, have not provided indications that organizations are preventing and protecting the enterprise from their adversaries.

Privacy

NIST 800-53 Revision 5 has fully embraced this notion by making a concerted effort to tightly integrate leading privacy practices throughout the broader 800-53 security control areas. This has broadened the focus of previous revisions — which were aimed at the protection of information, information systems, and by default organizations — to now also emphasize the protection of individual privacy data. At present, privacy programs at many organizations are often vague entities that are treated as an afterthought, or a check-the-box exercise, in terms of security. This is evidenced by the increasing number of privacy data breaches seen throughout the world today.

NIST 800-53 Revision 5 represents an excellent opportunity for organizations to get a better understanding of their privacy responsibilities as well as drive the behaviors necessary to properly identify and protect privacy assets within the natural course of the mission. **Organizations where chief information security officers (CISOs) and chief privacy officers (CPOs) currently operate separately now have a catalyst to drive integration between their teams and operate under one flag to better protect data.** Another opportunity presented by Revision 5 is for CISOs and CPOs to revisit system development life cycle (SDLC) and procurement practices to have a higher level of assurance that privacy concerns are embedded in both by design. CISOs and CPOs who actively embrace the opportunity to operate as one entity and weave privacy practices throughout organizational security controls — as prescribed by NIST 800-53 Revision 5 — have a higher chance of success in mitigating the threats to privacy that are common in today's mission environment.

Supply chain risk management

NIST 800-53 Revision 5 recently added an entirely new control family focused on supply chain risk management (SCRM). SCRM is a topic that has been brought to the forefront of many IT leaders in the federal government through federal requirements, such as the Federal Acquisition Supply Chain Act, the National Defense Authorization Act of 2019 (Section 889) and Executive Order 13873, along with industry-specific SCRM regulations, such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) 13. Not only has SCRM had legal and regulatory highlights recently, it is also a key area of risk for organizations, whereas 38% of organizations had a data breach caused by a supplier and 52% of organizations had an outage caused by a supplier — both over the past two years (EY Third-Party Risk Management 2019 survey). The inclusion of the SCRM control family will have direct impacts to the risk management framework (RMF) processes and will also challenge cyber professionals to integrate across organizational boundaries and broaden their risk aperture.

To incorporate SCRM within the RMF processes an organization first needs to align the RMF process to the supplier life cycle. Traditional RMF processes initiate after a product is purchased to select, implement, assess and monitor security controls; however, this is too late for SCRM risks as once a product is purchased, an organization has already accepted the risks associated with working with a supplier and their associated supply chain. To mitigate this, the RMF-associated SCRM processes should be embedded at the onset of a potential procurement to support supplier and supply chain risk assessment capabilities within the pre-procurement (market analysis) and procurement life cycles. By embedding the SCRM controls within the procurement processes, the security team will have visibility to supplier and supply chain risks to support helping leaders make risk-informed decisions, as well as have a starting point, based upon supplier assessments, to support system categorization and control selection.

Effectively reviewing a supplier and their associated supply chain significantly broadens the scope of RMF professionals beyond cybersecurity. In order to review a supplier and understand the risks they present to an organization, an RMF professional must be able to evaluate additional risk elements, such as financial, provenance (a product's supply chain), foreign interest, compliance and geopolitical risks. These additional risk elements provide the context required to evaluate the overall health of a supplier, their products and their supply chain prior to procurement. Additionally, SCRM goes well beyond that of a standard system going through the RMF process and should also broaden the scope beyond IT systems to now look at operational technologies, such as bulk electric systems (BES) and the internet of things (IoT) devices, as these devices often have a higher operational impact to an organization in the event they are compromised.

In brief

- Cybersecurity cannot be a paperwork exercise — it requires an integrated and effective testing strategy that allows for the NIST 800-53 Revision 5 testing results to be leveraged across different regulatory frameworks that are supported by quality-based evidence.
- Organizations where CISOs and CPOs currently operate separately now have a catalyst to drive integration between their teams and operate under one flag to better protect data.
- For an organization to be successful in their SCRM journey, the RMF processes need to be embedded within the procurement life cycle. Additionally, the security team should broaden their understanding of risk beyond cyber and they must establish cross-organization collaboration with cybersecurity, procurement, operational technology operators and enterprise risk management functions.

EY Cybersecurity teams can help organizations to:

- Help implement and execute a strategy and overarching cyber program that allows for rigorous, structured decision-making and a financial analysis of cyber risks
- Help EY clients achieve and sustain regulatory compliance requirements as the outcome of a well-designed and executed cyber function
- Stay up-to-date with leading services in data security and data privacy
- Help organizations assess their risk exposure across Tier 1 and 2 suppliers while helping them develop their predictive analytics capability and an integrated risk management approach.

Learn more

For more information on how EY can help, please contact:

Kris Lovejoy
EY Global Consulting
Cybersecurity Leader
kristin.lovejoy@eyg.ey.com

Dave Burg
EY Americas Consulting
Cybersecurity Leader
dave.burg@ey.com

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

US SCORE no. 10878-201US
2010-3597543
ED None

ey.com