Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

The IT Security budget is a zero-sum game, every dollar spent on compliance is a dollar not spent on risk-management. Therefore, balancing the need to deploy risk-appropriate security controls against deploying those mandated by regulatory or contractual obligations is one of the greatest challenges to improving cybersecurity practices.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

The diverse and unique needs between various sectors will mean that whatever framework is developed, it will have to focus on program-level risk management and not specific technical or administrative controls. If this is the case why re-invent the wheel and why not simply adopt ISO 27001 as a framework (already internationally accepted)?

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

Our information security policy is based on ISO 27001, and ITIL with many enterprise-specific policies added to acknowledge risk tolerance of company and architectural realities of environment. Senior management has governance oversight of security policy and directs the Information Security office for matters of communication and education.

4. Where do organizations locate their cybersecurity risk management program/office?

Corporate headquarters

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

There are several risk management organizations within the enterprise dealing with domain-specific threats and treatments. Information security is has developed it own risk-management methodologies including home-grown frameworks and well as industry frameworks such as OCTAVE and ISO 27005.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

It is addressed but not managed through the centralized risk management organization. The information security group is managed inside the IT organization.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

ISO 27001/2/5, ITIL, OCTAVE, OWASP, MS SDL, Common Criteria, PCI DSS, home-grown frameworks and techniques.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

SOX, HIPAA, FAA, TSA, PCI DSS, Privacy laws (local, state, international)

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

Transportation sector has dependencies on telecommunications, energy, information technology, and transportation entities within sector.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

Availability trumps confidentiality or integrity controls in transportation sector so there is a focus on service uptime and disruption minimization goals. Regulatory compliance is also a stated goal.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

An auditor letter of attestation is enough to satisfy most reporting requirements. Other information that may be shared; access logs samples, data flow diagrams, etc.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

Standards and frameworks are useful as guidance in building a program or comparing results but are incomplete since they do not address sector/business specific risk factors or treatments. An organization's risk tolerance for components and systems within an enterprise that are not critical for mission success cannot be treated the same as those that are critical to the mission. Many standards and frameworks miss this point and paint control requirements with a broad brush that increases costs but does not reduce risk.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

ISMS is based on ISO 27001, Operations based on ITIL, regulated data/system controls dictated by various laws and standards (SOX, PCI DSS, etc.)

2. Which of these approaches apply across sectors?

These approaches should work across all sectors since business risk is handled via ISO/ITIL inspired controls and prescriptive controls are defined by regulation/standard.

3. Which organizations use these approaches?

Many of the F500.

4. What, if any, are the limitations of using such approaches?

None, since they are modular and non-binding an organization can cherry-pick the parts that work, modify the parts that don't quite fit, or ignore other parts completely.

5. What, if any, modifications could make these approaches more useful?

Updated more regularly. More public discussion of frameworks and standards before they are published.

6. How do these approaches take into account sector-specific needs?

They do not. They are written in a way to allow organizations across many sectors to adopt the frameworks and standards as they see fit.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

That would be helpful to understand what other organizations within sector are doing (share common practices).

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

They could coordinate meetings and publish minutes and sector-specific standards that have been agreed upon by members of a ISAC and/or CIPAC.

9. What other outreach efforts would be helpful?

Pollination of common practices across several sectors. Publishing cross-sector dependencies and practices (such as Transportation depends on Telecommunications).

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

1. Are these practices widely used throughout critical infrastructure and industry?

Yes, we use all the practices listed.

2. How do these practices relate to existing international standards and practices?

ISO 27001 addresses these as part of the ISMS program.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

Mission/system resiliency practices; monitoring and incident detection tools and capabilities; identification and authentication.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

I don't see a case where a business wouldn't deploy these controls / processes somewhere in their organization.

5. Which of these practices pose the most significant implementation challenge?

Asset identification and management.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

ISO 27001 ISMS, ISO 27002, and ITIL establish these programs, practices, processes, and control types.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

Yes, enterprise architecture groups and the CTO office are instrumental in these functions.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

Yes.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Privacy and civil liberties are increased through the just application of these practices. Protecting stakeholder PII is critical to the success of a public company that depends on customer trust as an asset. Cryptographic, authorization, and audit controls become paramount in protecting privacy.

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

There are many. Cryptographic key management, personal data storage, transmission, and release are all issues that must be managed through on a case-by-case and country-by-country basis.

11. How should any risks to privacy and civil liberties be managed?

Ensure there are no provisions mandating warrantless release of personal data, ensure that aggregation is used when sharing information to sector members, scrub or replace personal data if included in an indicator of compromise (IOC).

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Governance & Policy