National Grid Overview

National Grid is an international electric and natural gas company and one of the largest investor-owned energy companies in the world. We play a vital role in delivering gas and electricity to millions of people across the northeastern United States and Great Britain in a safe, reliable and efficient manner.

Electricity Transmission – United States
National Grid owns and operates transmission facilities in upstate New York, Massachusetts, Rhode Island and Vermont in the United States. We also own and operate a 139 mile transmission line between New England and Canada.

Electricity Distribution and Generation- United States
National Grid owns distribution facilities used to provide electric service to 3.5 million end-use customers in upstate New York, Massachusetts, and Rhode Island.

National Grid Generation LLC, a National Grid subsidiary, also owns generating assets. In Calendar Year 2012, National Grid Generation LLC produced 5,266,117 MWh of electricity.

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?***

   Challenges to improving the cybersecurity of critical infrastructure begin with properly defining and scoping the threat and then identifying, classifying and tracking assets in an ever-evolving organization.

   Operational Technology is often comprised of closed systems warranted by system vendors only as long as customers configure and deploy systems using their rigid specifications. By in large, these system vendors focus on system availability rather than security, to the detriment of good security best practices. Vendor support staff can view security controls as inhibitors to effective operations.

Once the project team agrees on a solution, the business must support the investment. Quite often, the justification for improving cybersecurity lies in attempts to quantify risks in a complex eco-system.

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

National Grid sees the greatest challenge in developing a cross-sector standards-based Framework as the harmonization of existing approaches to compliance within different sectors, whilst still leveraging the people, processes and technologies deployed. National Grid has both electric and gas assets within our footprint. Each of these sectors adopts differing and incongruent approaches to cybersecurity.

Electric utilities take a prescriptive, rules-based, approach to cybersecurity in the form of mandatory NERC Critical Infrastructure Protection ("CIP") standards. Gas utilities are voluntary and principle-based with the adoption of the TSA Pipeline Security Guidelines. Finally, DHS takes a hybrid approach with the Chemical Facility Anti-Terrorism Standards. With operational cybersecurity standards alone, National Grid has three different approaches to cybersecurity with very little similarity in approach.

Because of the inherent differences between industries, a principles-based framework would be more beneficial than a rules-based framework.

At a high level, rules are sets of instructions with either a dichotomous (adhered to or not adhered to) or continuous (10%, 20%,…, 90%) compliance measure. Principles, on the other hand, are general statements that define a goal or objective of the entity adhering to the principle. In the case of information or cybersecurity, the main constituent of a principles based approach is a risk-based approach. Therefore, principles build in risk mitigation.

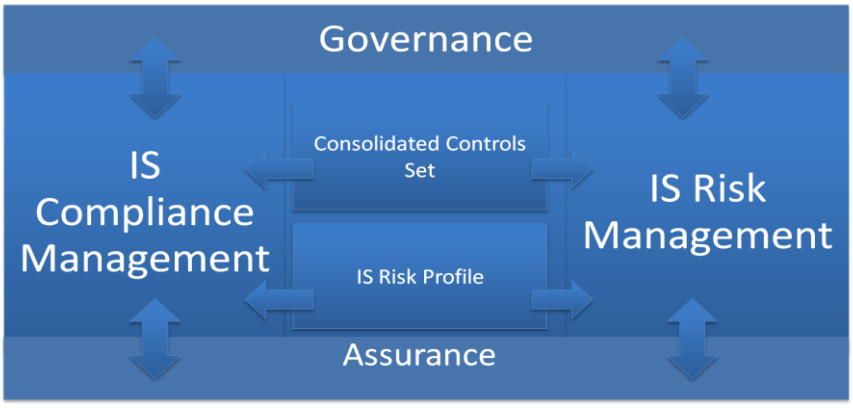
The main advantage of principles or risk-based approaches to regulation is that they cover a wider range of scenarios than rules-based approaches. However, principles devolve discretion to the entity and require guidance on the level of conservatism applied to their implementation. On the other hand, a rules-based regulatory system ensures that all parties that need to adhere to it are applying the same set of security controls and may go to the next level of detail as to specify how the controls are implemented. This can be seen as a 'double-edged' sword since all parties will have the same level of security, if there is a gap in the regulation, e.g. a particular aspect of security is missed, this will affect all parties in the same way and the systematic risk will be high. Alternatively, a risk-based system, where the individual parties identify the type of security controls that they will implement separately, ensures that the systematic risk is lower.

It is important to note here that both a risk based and rules based regulatory frameworks could require completion of a risk assessment but the specific requirements around how it is done and applied to the business are likely to be different.

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?

National Grid's Digital Risk and Security organization consists of teams focused on security architecture and design, security policy, security project management, data privacy, compliance management, risk management, threat management, incident management, security consultancy and privacy. These teams all work together to develop and refine policies and standards, and protect information based on data privacy and critical infrastructure considerations in accordance with the law and data classification. Additionally, the Digital Risk and Security organization identifies threats and vulnerabilities, implements controls to mitigate risks, and manages residual risks via the risk register and profile. Finally, the Digital Risk and Security organization aligns compliance objectives with regulatory, legal and statutory obligations and requirements and provides assurance and attestation of their effectiveness.

National Grid utilizes a standardized approach to I.S. Governance, Risk and Compliance regardless of the domain, including operational, physical security, cyber security, privacy and resiliency.



<u>Program Governance</u>

A robust multi-level governance framework exists within National Grid to help provide oversight for IS Risk and Compliance activities.

IS Risk Committee

The IS Risk Committee consists of the IS Leadership Team, Chief Information Officer, Chief Information Security Officer, IS Audit, Corporate Risk Management and Corporate Resiliency and is responsible for providing oversight of the IS Risk and Compliance program.
The committee maintains an understanding of all risks agrees to and approves National Grid's response to high risks, and makes reporting recommendations for Board-level risk and compliance issues.

Three subordinate working groups exist to support the IS Risk Committee. Those groups are:

Policy & Standards Governance Board (Co-Chaired with Enterprise Architecture)

The Policy & Standards Governance Board is a forum that provides the opportunity to discuss and approve National Grid IS Policies and Standards. Its focus is to collaboratively develop and maintain the IS Policies and Standards such that they complement and reinforce each other.

Risk Working Group

The Risk Working Group is a forum that provides the opportunity to discuss existing IS risks and any new IS risks that are brought forward for possible inclusion in the risk register. The Risk Working Group will review the corresponding proposed actions, due dates, and action owners in order to determine if these potential risk mitigation efforts are sufficient.

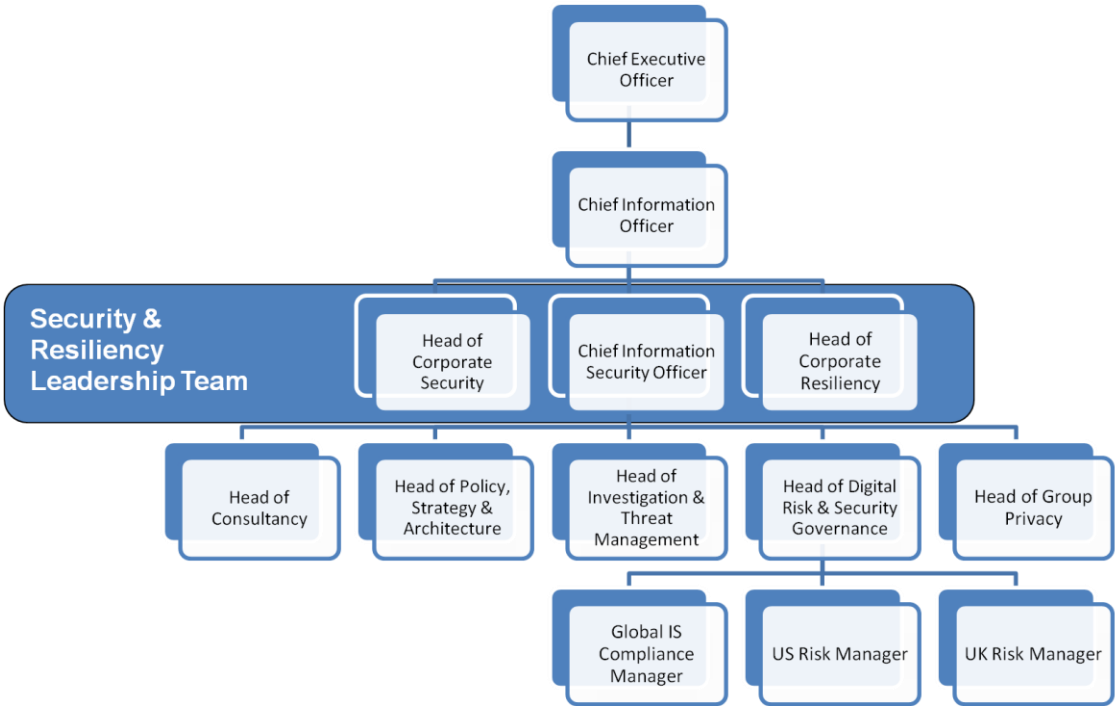
Compliance Working Group

The IS Compliance Working Group is a forum that provides the opportunity to discuss National Grid compliance with internal and external controls. Its focus is to sustain a compliance program that will ensure the effectiveness of IS controls.

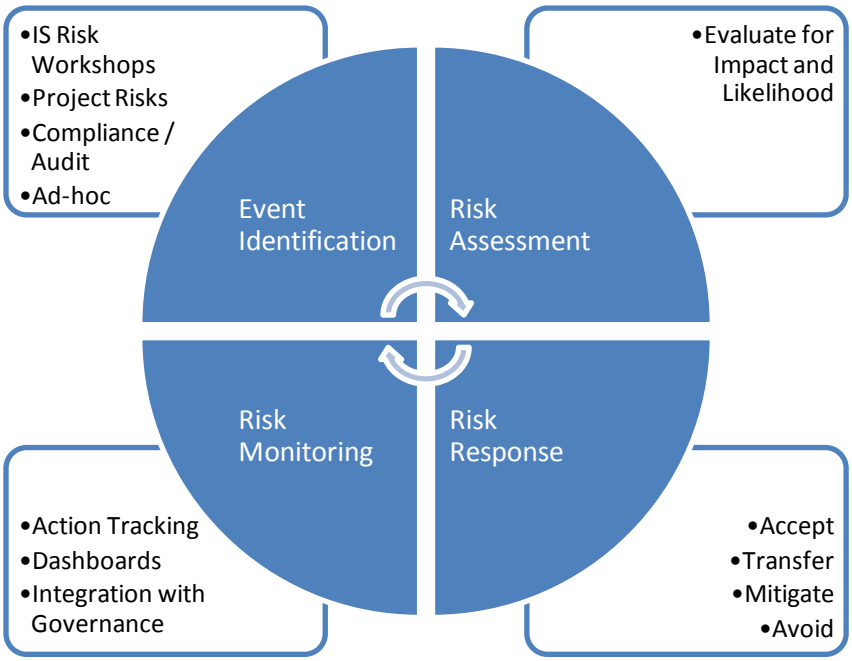
4. Where do organizations locate their cybersecurity risk management program/office?

Digital Risk & Security

National Grid cybersecurity risk management is part of the IS Risk Management program and IS Risk Management is embedded within the Digital Risk & Security team. Even though the function is part of the Digital Risk & Security team, the scope of the team includes all areas of IS Risk including risks related to critical infrastructure.



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



Risk Identification

National Grid offers several formal and informal mechanisms to identify and report risk within the estate.

- **Risk Workshops** – IS Risk Management conducts regular workshops with all functional areas within Information Services (including the Critical National Infrastructure Support Team). These workshops are brainstorming sessions where leadership collaborates to create a list of risks that are most concerning to them.
- **Project Risk Assessments** – Project work within National Grid often brings change to the control environment resulting in a potential risk to National Grid. These risks are managed via the risk management process.
- **Internal Compliance / Controls Assessments** – National Grid IS Compliance performs regular assessments of the control environment within National Grid's assets. Any deviation from established controls represents a potential risk to National Grid and are inputs into the IS Risk Management process.
- **Internal / External Audits** – Internal / External audits often result in a list of deficiencies or observations. These observations represent a potential risk to National Grid and are inputs into the IS Risk Management process.
- **Ad-hoc Risk Reporting** – Risk Management is the responsibility of every National Grid employee and contractor. The ad-hoc risk reporting process offers individuals the opportunity to raise potential risks for consideration as inputs into the IS Risk Management process.

Risk Assessment

National Grid scores risk utilizing a 5-point scale related to Financial Impact (including operational impacts and risks), Reputational Impact, and Likelihood. The score is then multiplied together (Largest Impact x Likelihood) to create a standardized score. There are both quantitative and qualitative measures available depending on which is easier to gauge.

Risk Response

National Grid evaluates the risk assessment and agrees on an appropriate response. All risks require approval by a business and IS risk owner. The level of signoff differs based on the degree of risk presented to the organization. Once the risk response is agreed, the risk management team enters the risk and appropriate action plan into the risk register for ongoing monitoring.

National Grid uses the standard COSO risk management model. Acceptable risk response includes Accept, Transfer, Mitigate and Avoid.

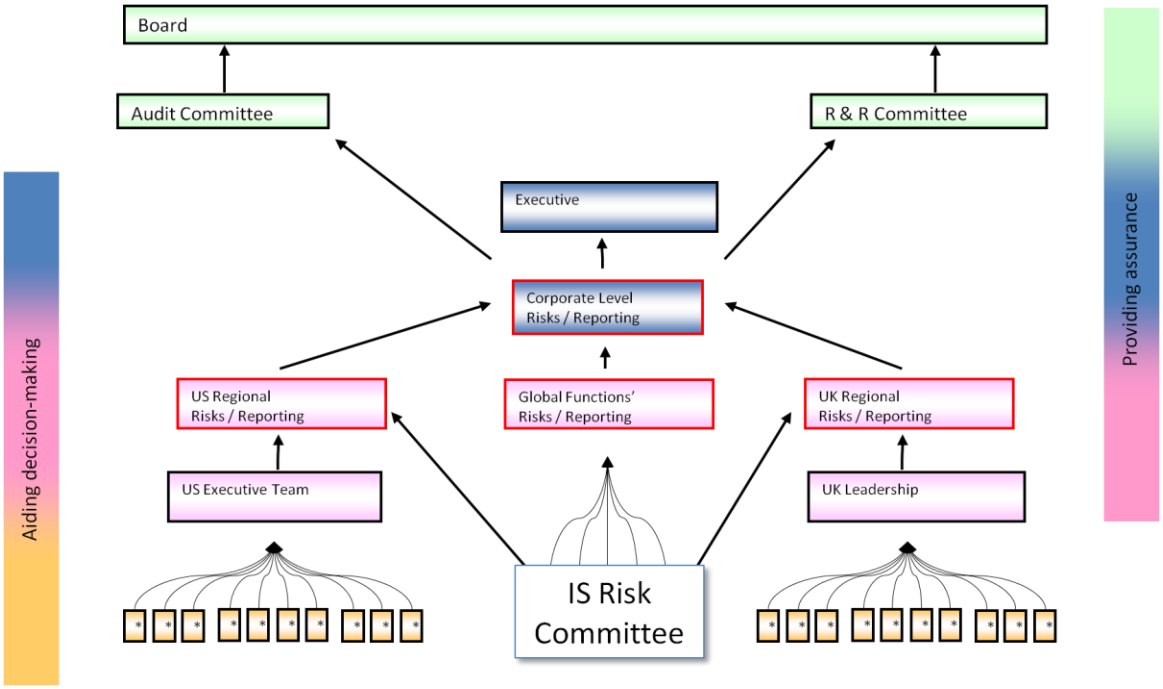
Risk Monitoring

IS Risk Management maintains the risk register and agreed risk actions. National Grid tracks the status of all risk actions and updates the actions and risk register as necessary. Dashboards and reports exist to provide IS leadership and Corporate Risk Management a view of the IS Risk Profile via the established governance process.

The IS Risk profile is used as an input to the IS Strategy, Assurance and Governance processes.

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

IS Risk Management as a function fully manages the risk profile within IS, but provides visibility of major risks to the business and board via reporting to the Corporate Risk Management process.



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

The National Grid IS Risk Program is based on the COSO framework and is fully integrated with the IS Compliance program, IS Internal Audit, External Audit, Vendor Assurance (Outsourcing Risks), and SDLC (Project Risks). National Grid has selected RSA Archer eGRC Suite as the eGRC toolset.

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?

- NERC Critical Infrastructure Protection Standards
- Department of Homeland Security, Chemical Facility Anti-Terrorism Standards
- Transportation Security Administration, Pipeline Security Guidelines
- PCI Data Security Standards
- SOX – IT General Controls / Entity Level Controls
- HIPAA / HITECH
- MA Privacy Act
- New York – Department of Public Service

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

National Grid's is interdependent on other energy producers and interconnected utilities. In addition, National Grid SCADA and Energy Management systems are dependent on telecommunications sector assets to provide near real-time status and control. Finally, operation and maintenance of the critical assets requires the use of roads and transportation assets.

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

National Grid's governance process measures and reports on key performance indicators and key risk indicators. In addition to operational IS metrics, National Grid reports on key security metrics related to email, anti-virus / anti-spyware, firewall / network perimeter, attacks, patch management, host configuration, vulnerability management, training & awareness and compliance & governance.

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?***

    National Grid provides proactive compliance attestations to multiple jurisdictions in the United States covering NERC CIP, PCI-DSS, Sarbanes Oxley, CFATS and TSA Pipeline centered on National Grid's Information Security Management program and the effectiveness of the controls.

    National Grid participates in third party assessments, of the same information security management controls, conducted by NPCC, NY-DPS, PwC, KPMG and DHS on a regular basis related to NERC CIP, Sarbanes Oxley, CFATS and TSA Pipeline.

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

    National/international standards and organizations should provide high-level baselines and documented best practices for implementing successful information security and risk management programs. Additionally, standardization should provide a structured taxonomy and rigid data dictionary to support interfaces and information sharing between disparate organizations with customized internal information security and risk management programs.

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?***

   Critical Infrastructure Specific

- NERC Critical Infrastructure Protection
- TSA Pipeline Security Guidelines
- DHS Chemical Facility Anti-Terrorism Standards
- NIST Smart-Grid

Process Specific Standards

- Payment Card Industry – Data Security Standards
- HIPAA / HITECH

General Information Security Standards

- NIST 800-53
- ISO 27000
- CobIT

2. *Which of these approaches apply across sectors?*

- NIST 800-53
- ISO 27000
- CobIT

3. *Which organizations use these approaches?*

National Grid makes use of all applicable standards and regulations through a risk-based process of harmonizing and mapping controls to form a tailored control set that is specific to National Grid. The consolidated control set (169 controls) forms the foundation for National Grid compliance and risk management program.

Benefits to this risk-based harmonized approach include:

- Standardized control set with interface to risk drivers
- More efficient management of the complex compliance environment
- Test results can be linked to multiple overlapping requirements (i.e., test once and apply to many)
- Single-source of information and reporting for high-level management
- Reduced operational risk exposure
- Reduced overall compliance and audit costs

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

The rules-based, standards approach addresses the existing, known threat landscape but does not foster or promote future or emerging threats. The governance process that is required to evaluate threats, assess risks, identify and implement controls (process and technology) can be cumbersome and time-consuming.

At a high level, rules are sets of instructions with either a dichotomous (adhered to or not adhered to) or continuous (10%, 20%,…, 90%) compliance measure. Principles, on the other hand, are general statements that define a goal or objective of the entity adhering to the principle. In the case of information or cybersecurity, the main constituent of a principles based approach is a risk-based approach. Therefore, principles build in risk mitigation.

The main advantage of principles or risk-based approaches to regulation is that they cover a wider range of scenarios than rules based approaches. However, principles devolve discretion to the entity and require guidance on the level of conservatism applied to their implementation. On the other hand, a rules based regulatory system ensures that all parties that need to adhere to it are applying the same set of security controls and may go to the next level of detail as to specify how the controls are implemented. This can be seen as a 'double-edged' sword since all parties will have the same level of security, if there is a gap in the regulation e.g. a particular aspect of security is missed, this will affect all parties in the same way and the systematic risk will be high. Alternatively, a risk based system, where the

individual parties identify the type of security controls that they will implement separately, ensures that the systematic risk is lower.

It is important to note here that both a risk based and rules based regulatory frameworks could require completion of a risk assessment but the specific requirements around how it is done and applied to the business are likely to be different.

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

National Grid proposes a framework that includes a collaborative approach between Government, Industry and Solution Providers.

Cybersecurity Framework

Develop a Cybersecurity Framework that addresses the clear need for minimum processes and controls within any critical infrastructure provider at a baseline level. Make allowance for changes to the framework based on risk assessments (mitigating or compensating controls).

> **Example:**
> *Documented Policies, Asset Identification, Periodic Risk Assessment, Logging, Patch Management, and anti-virus / malware*.

Explicit Standards for Shared Interfaces

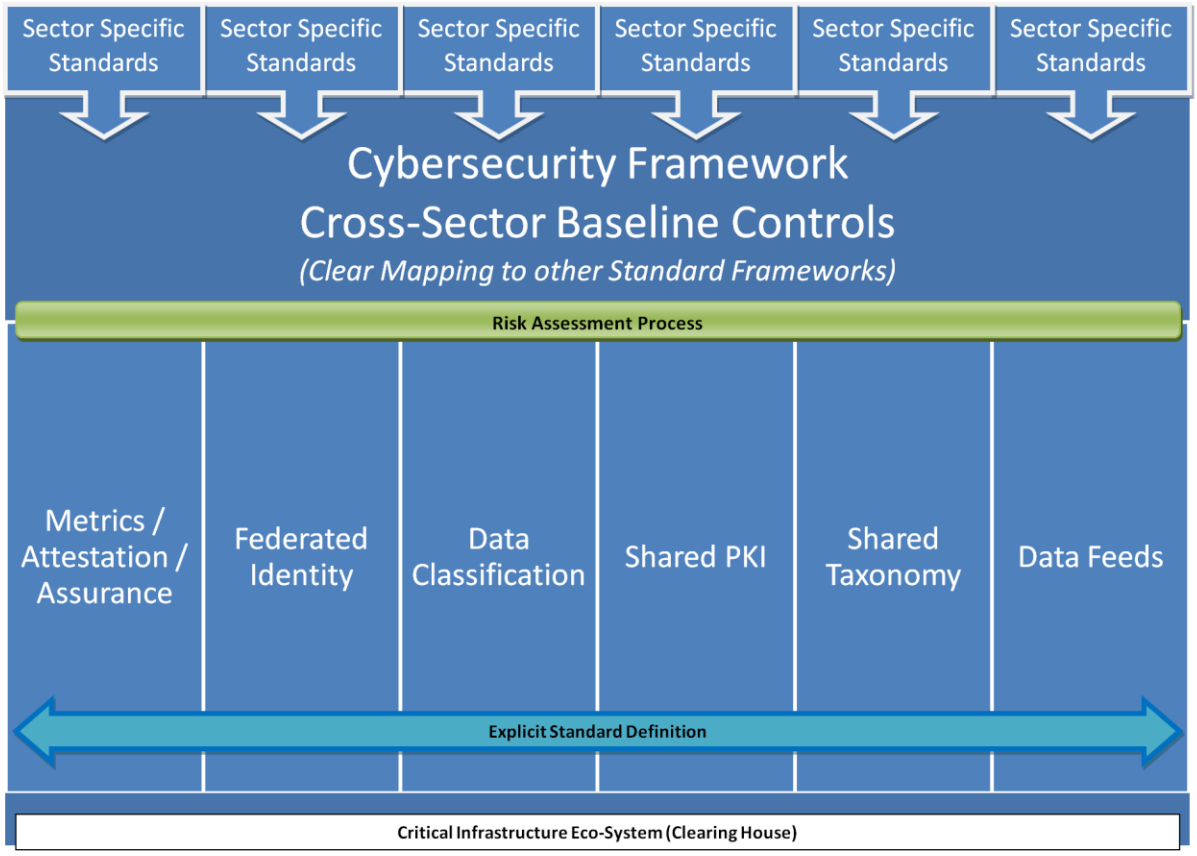
Explicit standards are required to enable information-sharing and assurance within the eco-system. If done properly, these standards will enable industry participants as well as system vendors to create compliant solutions for information sharing.

> **Example:**
> *Firewalls, IDS/IPS Systems, Log Collectors, applications and operating systems could have reporting modules that would send encrypted anonymous log data to a centralized clearinghouse for data mining and evaluation.*

Snap-In capability for Sector-Specific Standards

Recognizing that there are specialized technologies that are critical to specific sectors, National Grid proposes the development of a list of snap-in or ala carte standards around each individual technology. Industry participants can choose to integrate each standard into their framework as the result of their risk assessment. As a value add proposition, vendors can certify their systems as compliant with the standard, thus reducing the level of effort by the industry participant.

Example:
Many industry participants across multiple sectors use SCADA systems to manage their industrial control systems. SCADA vendors would go through a certification process to show that their system is Compliant. When making purchasing decisions, industry participants would know that their system would meet all the standard requirements.



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

The framework should allow for sector-specific standards but rigid controls are required to ensure that sector-specific standards work cooperatively with rather than overlap or undermine the framework. There is a risk that sector-specific agencies would use sector-specific standards to circumvent the framework governance process defeating the advantages of a single cooperative framework.

Example:

Assuming that the baseline controls account for identity and access management, sector-specific standards should not address specify password complexity requirements.

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

   The development team should make every effort to address the fundamentals of a good cybersecurity program through cross-sector standards. In the cases where this is not possible, the development team should only consider a sector-specific standard where a standardized approach is beneficial to the eco-system or required for information sharing.

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

   Sector-specific agencies are most familiar with critical industries within their jurisdiction and therefore should play a significant role in sector-specific standard development. Overall framework development and alignment should remain the domain of NIST with input provided by all who wish to contribute.

9. ***What other outreach efforts would be helpful?***

   National Grid encourages NIST and other agencies to reach out to the international community in an effort to devise a framework that is congruent with other standards so that entities that operate internationally can minimize conflicting cyber requirements.

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?***

   National Grid integrates each of these practices in our internal control framework based on previously listed international standards and best practices. Applicability of the controls to individual technologies is dependent on the outcome of a risk assessment in the environment.

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

   With the exception of privacy and civil liberties protection, each of the international standards and practices mentioned above include the tenants of these practices to varying degrees. Stand-alone standards and practices exist in the area of privacy and civil liberties protection.

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

   National Grid believes that asset identification and management is the most critical for secure operation of critical infrastructure. Any risk-based approach relies on the ability to understand scope and boundaries related to the system in question.

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

   National Grid integrates each of these practices in our internal control framework based on previously listed international standards and best practices. Applicability of the controls to individual technologies is dependent on the outcome of a risk assessment in the environment.

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

   Many utilities use highly complex, legacy systems that do not support these practices. Due to these limitations, National Grid has experienced varying degrees of success with identification and authorization of users accessing systems, monitoring and incident detection capabilities. In addition, the complexity related to implementing encryption and key management in highly available, operational systems is significant. In all cases, National Grid takes a risk-based approach to evaluate the threat and agree on an appropriate response.

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

   National Grid consults standards and guidelines when building out architectural patterns and solution design, but only as appropriate to National Grid's business requirements.

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

   National Grid's governance process provides a methodology for creation and management of IT standards. The methodology includes not only review and approval of new IT standards, but takes further steps to identify cost related to the implementation of standards prior to approval.

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

   National Grid's risk management process has a built-in escalation process based on risk severity. The Incident Management process is applicable in cases where a risk is immediate and severe. The Incident Management process is able to move quickly through and around typical governance process requirements.

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

   National Grid expects that information-sharing will be a pillar of the proposed Cybersecurity Framework. The framework must take special precautions to protect the anonymity of participants and their customers.

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

    National Grid is an international organization bound by laws in jurisdictions outside of the United States. The European Union has issued similar directives in the area of cybersecurity. National Grid strongly encourages the two regulatory bodies to work together to create a framework that is cooperative.

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

    National Grid advocates a risk assessment and thoughtful response to any risk. Privacy and civil liberties risks are no different from any other risk.

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

    National Grid believes that a comprehensive cybersecurity framework should also consider training and awareness, information handling, and metrics and assurance.