## 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?

While information security and cybercrime are known and discussed at board level, these activities are often not aligned sufficiently with other business efforts and risk management practices. Despite the increase of breaches and cybercrime, additional resourcing and security personnel are not a priority for many.

With budgeting and investment in new technologies and systems remaining a challenge for many organizations, the opportunity to innovate and utilize resources remains limited.
While a number of organizations appear to be targeting specific areas, few are taking a holistic approach encompassing people, processes and technology. Each component is as vital as the next, and this is a delicate balance which will need to be achieved moving forward into 2013.
*~ Deloitte, in association with EMC, first annual Information Security and Cybercrime Survey~*

In today's rapidly evolving "threat" landscape, many R&C businesses have fallen behind with the result that with tight budgets and truncated projects security practices have been weakened. At the same time, their adversaries are becoming ever more sophisticated, breaching the defenses of business ecosystems and leaving reputational, financial, and competitive damage in their wake.
Those keeping score agree: The adversaries appear to be in the lead.

For too many businesses, budgets are not keeping pace with changes in enterprise systems, which may jeopardize their ability to gain and maintain competitive advantages. New technologies are being adopted faster than they can be safeguarded. And senior executives frequently are seen as not always supportive of increased spending as the solution.

Retail & Consumer Insights - www.pwc.com/us/retailandconsumer

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

Buy-in from Management. While most CEOs see cyber threats as a concern, they still see actions and resources needed as low priority VS activities that increase profit. They also see this a threat to their independence.

As referenced in the recent survey issued by Jay Rockerfeller, "many companies raised concerns about any new federal program that would set mandatory cybersecurity requirements, create obligations that would impact their ability to address cybersecurity issues in a **flexible**" (Commentary: this is CEO speak for doing as little as possible) "manner or duplicate efforts already underway".

### 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?

We have a structured process developed under ISO 27001 as follows:

We defined an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that:

1) includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;

2) takes into account business and legal or regulatory requirements, and contractual security obligations;

3) aligns with the organization’s strategic risk management context in which the establishment and maintenance of the ISMS will take place;

4) establishes criteria against which risk will be evaluated ; and

5) has been approved by management.

c) Defined the risk assessment approach of the organization.

1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.

2) Developed criteria for accepting risks and identify the acceptable levels of risk.

d) Identify the risks.

1) Identified the assets within the scope of the ISMS, and the owners of those assets.

2) Identified the threats to those assets.

3) Identified the vulnerabilities that might be exploited by the threats.

4) Identified the impacts that losses of confidentiality, integrity and availability may have on the assets.

Note The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ’owner’ does not mean that the person actually has any property rights to the asset.

e) Analyzed and evaluated the risks.

1) Assessed the business impacts upon the organization that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.

2) Assessed the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

3) Estimate the levels of risks.

4) Determine whether the risks are acceptable or require treatment using the criteria for accepting risks

f) Identified and evaluated options for the treatment of risks.

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organization’s policies
and the criteria for accepting risks

3) avoiding risks; and

4) transferring the associated business risks to other parties, e.g. insurers, suppliers if applicable.

g) Select control objectives and controls for the treatment of risks.

Control objectives and controls are selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection takes account of the criteria for accepting risks as well as legal, regulatory and contractual requirements.

The control objectives and controls from Annex A of ISO 27001 are selected as part of this process as suitable to cover the identified requirements.

The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

h) Obtain management approval of the proposed residual risks.

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

Typically it is located at the designated enterprise headquarters of the organization.

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

Most common are the guidelines as specified by ISO/IEC 27001. They are as follows:

1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.

2) Developed criteria for accepting risks and identify the acceptable levels of risk.

d) Identify the risks.

1) Identified the assets within the scope of the ISMS, and the owners of those assets.

2) Identified the threats to those assets.

3) Identified the vulnerabilities that might be exploited by the threats.

4) Identified the impacts that losses of confidentiality, integrity and availability may have on the assets.

Note The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.

e) Analyzed and evaluated the risks.

1) Assessed the business impacts upon the organization that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.

2) Assessed the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

3) Estimate the levels of risks.

4) Determine whether the risks are acceptable or require treatment using the criteria for accepting risks

f) Identified and evaluated options for the treatment of risks.

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policies
and the criteria for accepting risks

3) avoiding risks; and

4) transferring the associated business risks to other parties, e.g. insurers, suppliers if applicable.

g) Select control objectives and controls for the treatment of risks.

Control objectives and controls are selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection takes account of the criteria for accepting risks as well as legal, regulatory and contractual requirements.

The control objectives and controls from Annex A of ISO 27001 are selected as part of this process as suitable to cover the identified requirements.

The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

h) Obtain management approval of the proposed residual risks.

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

It is a living breathing part of the overall information security management system that addresses all aspects of People, Process and Technology.

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

There are many out there, few internationally renowned. Most popular are, ISO/IEC 27001, ISO/IEC 20000-2011, COBIT, ISO 31000, ISO 27031

**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?**

State governments have attempted to improve cyber-security by increasing public visibility of firms with weak security. In 2003, California passed the Notice of Security Breach Act which requires that any company that maintains personal information of California citizens and has a security breach must disclose the details of the event. Personal information includes name, social security number, driver's license number, credit card number or financial information. Several other states have followed California's example and passed similar security breach notification regulations. These security breach notification regulations punish firms for their cyber-security failures while giving them the freedom to choose how to secure their systems. Also, this regulation creates an incentive for companies to voluntarily invest in cyber-security to avoid the potential loss of reputation and the resulting economic loss that can come from a successful cyber-attack.

In 2004, California passed California Assembly Bill 1950 which also applies to businesses that own or maintain personal information for California residents. This regulation dictates that businesses maintain a reasonable level of security and that these required security practices also extend to business partners. This regulation is an improvement on the federal standard because it expands the number of firms required to maintain an acceptable standard of cyber-security. However, like the federal legislation, it requires a "reasonable" level of cyber-security, which leaves much room for interpretation until case law is established.

All current state laws can be found here: [http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx](http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx)

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

Each organization is different. It is not a "one size fits all" answer. You must assess the business impacts upon the organization that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets. Then assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.

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

Everything traces back to the objectives of the organization. Typically Management will provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) establishing an ISMS policy;

b) ensuring that ISMS objectives and plans are established;

c) establishing roles and responsibilities for information security;

d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;

At that point, they will then define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results.

Then management will undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.

**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?**

All relevant statutory, regulatory and contractual requirements are reviewed and documented and the approach to meet these requirements are explicitly defined, documented, and kept up to date for each information system and the organization.

Appropriate procedures are implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary products.

Records are established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS and to be available for regulatory agencies. They are protected and controlled.

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

They should play a very critical role. This International Standards adopt a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS.

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

In order to protect and monitor our critical infrastructure properly, there needs to be a certain amount of transparency and consistency in the approach to continuous monitoring.

The process approach for information security management presented in International Standards such as ISO/IEC 27001 encourages its users to emphasize the importance of:

a) understanding an organization’s information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls to manage an organization's information security risks in the context of the organization’s overall business risks;

c) monitoring and reviewing the performance and effectiveness of the ISMS; and

d) continual improvement based on objective measurement.

Most standards use the Plan, Do Check Act model (PDCA) which is applied to structure all ISMS processes and takes inputs from the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations.

The adoption of the PDCA model also reflects the principles as set out in the OECD Guidelines (2002)1) governing the security of information systems and networks. Standards provide a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

## 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.

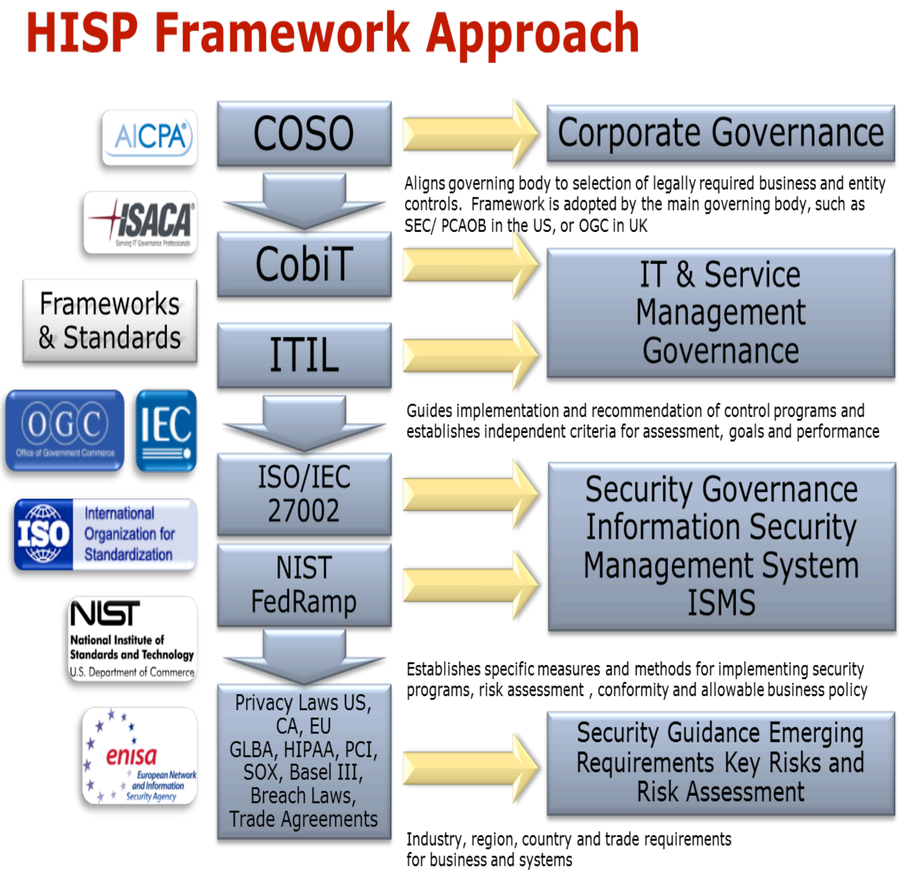
NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. ***What additional approaches already exist?***

There are many popular standards and frameworks used today in an attempt to promote the protection of information and information systems supporting organizational missions and business functions. Those frameworks are listed in the graphic below with an explanation of the areas of business they profess to address.

The Holistic Information Security Practitioner (HISP) integrated framework approach utilizes the Implement-Once-Comply-Many (I-O-C-M) philosophy based on a unique approach that stands alone in the security and compliance industry. I-O-C-M is a proven structured approach for solving business and compliance problems. This structured approach includes a powerful methodology, analytical methods and tools, improvement techniques and trained, capable people.

Many organizations struggle and treat each of their compliance requirements as a silo. By taking this approach, the opportunity for a security breach is increased. An integrated framework approach can help form the basis for a fully functional and secure information security program, as well as design and deploy a comprehensive risk governance platform for both compliance and assurance.


HISP Framework Approach
AICPA
ISACA
Frameworks & Standards
OGC
Office of Government Commerce
IEC
ISO
International Organization for Standardization
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
enisa
European Network and Information Security Agency
COSO
CobiT
ITIL
ISO/IEC 27002
NIST FedRamp
Privacy Laws US, CA, EU GLBA, HIPAA, PCI, SOX, Basel III, Breach Laws, Trade Agreements
Corporate Governance
Aligns governing body to selection of legally required business and entity controls. Framework is adopted by the main governing body, such as SEC/ PCAOB in the US, or OGC in UK
IT & Service Management Governance
Guides implementation and recommendation of control programs and establishes independent criteria for assessment, goals and performance
Security Governance Information Security Management System ISMS
Establishes specific measures and methods for implementing security programs, risk assessment , conformity and allowable business policy
Security Guidance Emerging Requirements Key Risks and Risk Assessment
Industry, region, country and trade requirements for business and systems

The Holistic Information Security Practitioner Institute (HISPI) is an independent certification organization that provides training and professional certification in the integration of best practices for enterprise and cloud information security management, auditing and compliance requirements. HISPI promotes a holistic approach to information security program management.

HISPI certified practitioners leverage the HISP Framework to provide a holistic, all-encompassing integrated management system that will greatly improve efficiency, reduce waste and cut costs.

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

While many claim to apply across all sectors, ISO 27001 and NIST are really the only two that are not sector specific and are scalable across many sectors by themselves. This is because they are harmonized with each other. The other frameworks have some similarities but address a more specific part of the business. The HISP Framework is an integrated best practice framework approach that teaches and guides organizations on how all the specific standards can be applied across all industry sectors to provide a more robust, holistic and secure environment.

### *3. Which organizations use these approaches?*

COSO is more related to the accounting industry, COBIT and ITIL are specific to the IT industry. ISO 27001/27002 and NIST/FEDRAMP are more broad in nature, not specific to any sector and harmonized with each other. The HISP Framework approach brings all of these frameworks together and has been delivered to security practitioners on a global scale. Many of the Top 10 organizations in the following industry verticals:

Accredited Certification Body
Consulting
Energy
Engineering
Financial Services
Healthcare
Higher Education
Legal
Manufacturing
Media
Public Sector (Federal, State and County)
Retail
Software
Telecommunication
Transportation

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

Individually COSO, ITIL and COBIT all have certain limitations because they are very sector focused as described in question 3 and don't address the wider business community, thus not allowing for organizational wide risk management. ISO 27001 is considered more of an umbrella standard that maps to all the other standards thus allowing for a more organizational wide consistent system and is the foundation the HISP framework is built off of. The HISP Framework approach teaches how to minimize those limitations because it is a best practice that is agile, fluid and elastic, encompassing numerous frameworks, methodologies, and global best practices. The HISP Framework is anchored in the continuous improvement process, and can adapt to any situation and addresses any industry vertical.

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

The best approach would be to harmonize the individual sector specific frameworks under one holistic standard like ISO 27001. This approach has been proven to be effective in mitigating Cybersecurity threats over the past 8 years.

The table to the right depicts for 2012 the HISPI Top 20 ISO 27001 Mitigating controls which allow organizations to mitigate against known real world Cybersecurity threats that have been exploited, resulting in the loss of confidentiality, integrity and availability of information assets.

| ***2012 HISPI Top 20 ISO 27001 Mitigating Controls*** | | |
|---|---|---|
| ***Ranking*** | ***Control*** | ***Number of Times Control Mapped to a Real-World Security Breach*** |
| **1** | A.10.9.1 | 447 |
| **2** | A.10.9.2 | 447 |
| **3** | A.10.9.3 | 447 |
| **4** | A.8.2.2 | 184 |
| **5** | A.7.2.1 | 94 |
| **6** | A.7.2.2 | 94 |
| **7** | A.8.1.1 | 90 |
| **8** | A.8.1.2 | 90 |
| **9** | A.8.1.3 | 90 |
| **10** | A.8.2.1 | 90 |
| **11** | A.8.3.2 | 90 |
| **12** | A.8.3.3 | 90 |
| **13** | A.9.2.5 | 87 |
| **14** | A.11.7.1 | 87 |
| **15** | A.11.7.2 | 87 |
| ***16*** | A.9.1.1 | 50 |
| **17** | A.9.1.2 | 50 |
| **18** | A.9.2.1 | 50 |
| **19** | A.10.8.4 | 16 |
| **20** | A.10.8.3 | 15 |

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

The HISP Framework approach takes into account industry/sector specific needs by allowing any organization to map its unique legal, contractual and regulatory compliance requirements to the HISP Framework approach.

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

The International Standards Organization (ISO) has had a standards development process in place for decades and is well accepted around the world. Actually NIST works closely with the ISO concerning the development of ISO 27001. Standards like ISO 27001 while are holistic in nature are designed to be flexible and scalable to any sector but provides an organizational wide, integrated approach that addresses People, Process and Technology. The HISPI advocates the use of a voluntary "integration program" rather than sector-specific standards. Cybersecurity threats relate to the loss of confidentiality, integrity and availability of information assets, irrespective of the sector that is impacted by the threat being realized.

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

N/A – please see response provided to Question 7.

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

Conduct outreach in the form of public meetings to help in the development of recommendations to improve the information security management process. Possibly separate events to solicit input. The first meeting, more of a Roundtable discussion with company CEOs, Information security and standards experts. The second should be a series of meetings (road show), and should include a much broader participation from the business community, academia, industry sectors, and the general public.

## 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?**

According to the SANS SCADA and Process Control Security Survey[1] conducted by the SANS institute, the use of these practices throughout the industries that host or support critical infrastructure is fragmented with some practices being heavily used and others nearly non-existent. The data, collected from nearly 700 participants across the major industries, states that roughly over half of the organizations participate in asset identification and management, monitoring and log analysis, and identification and authorization of users accessing systems. However, the vast amount of companies reported that they are not familiar with and do not implement the separation of business systems and networks from the areas where operations take place. Since there is no true separation between the two areas the average employee can reach systems responsible for controlling or automating critical infrastructure. Another area of slow adoption across the industry has been the implement of security engineering best practices as defined by the Systems Security Engineering Capability Maturity Model[2] (SSE-CMM). While many did map their security controls to widely known standards such as NERC CIP or the 20 Critical Security controls, many of these standards do not require a quantification of risk or a determination of acceptable levels of risk.

[1] http://www.sans.org/reading_room/analysts_program/sans_survey_scada_2013.pdf
[2] http://csrc.nist.gov/nissc/2000/proceedings/papers/916slide.pdf

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

With the exception of privacy and civil liberties protection, the practices described above are present in fragmented fashion across the most popular existing standards. The most popular standards for organizations that own or support critical infrastructure include: NERC CIP[3], ISA99[4], 20 Critical Security Controls[5], NIST Guide to SCADA and Industrial Control Systems Security[6], and the Chemical Facility Anti-Terrorism Standards[7]. Among the lesser implemented standards are ISO 27001[8], NRC[9], DoD specifications, and the Australian Security Standards. These standards vary in their breadth versus depth approaches to cyber security and their methodologies and attitudes towards risk management. As an example, the 20 Critical Security Controls is a surface level list of mostly technological requirements including malware protection, wireless device control, and boundary defense. While this is effective in some sense it does not truly all the risks that an organize faces. There are broad and flexible frameworks that are different in their approaches to cyber security because they deep dive into the area of risk management with an emphasis on risk awareness from the top levels of the organization to the bottom while still requiring the administrative, technological, and physical security controls that other frameworks demand.

[3] http://www.nerc.com/page.php?cid=2%7C20
[4] http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
[5] http://www.sans.org/critical-security-controls/
[6] http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20(2007).pdf
[7] http://www.dhs.gov/chemical-facility-anti-terrorism-standards
[8] http://www.bsigroup.com/en-US/iso-27001-information-security/
[9] http://www.nrc.gov/about-nrc/regulatory/research/digital/key-issues/cyber-security.html

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

Since we believe that cyber security needs to be approached in a holistic, realistic, and risk-based fashion we believe that the most critical practice to promote to the various critical infrastructure sectors is the security engineering practices. A proper implementation of best security engineering practices involves the understanding of security risks through assessments, an establishment of the security needs of the organization, the development of guidance related to security, determination of acceptable risk and risk levels, and the establishment of assurance of risk mitigation for the firm. This comprehensive and iterative approach allows the organization to systematically increase their security posture and assurance that they are prepared for cyber security attacks. Moreover, this general framework approach allows the organization to easily align their cyber security strategy with its business goals and objectives. This important fact creates an environment where cooperation and collaboration between stakeholders at all levels of the organization including management is required.

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

We believe all of these practices are applicable in some form or fashion to all critical infrastructure sectors as defined in table 2 of the GAO Report to Congressional Requestors on Critical Infrastructure Protection [10].

[10] http://www.gao.gov/assets/590/587529.pdf

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

The most significant implementation challenge of the above listed practices is the implementation of proper security engineering. We believe this to be the case because it implies that the administrators of critical infrastructure fundamentally change their approach to cyber security and their attitudes towards risk and risk management. The current mentality concerning risk across these organizations and industries is one of surface level remediation tactics and a misconception about the true risk that they face during every day operations. Moreover, there is a pervasive misconception about the potential consequences that organizations face if risk is left to flounder and a security event takes place. The movement towards a true security engineering framework and the implementation of that framework will bring with it plenty of challenges for organizations that do not want to change their attitude towards this fact and those that are aware of the risk but do not budget the appropriate resources to mitigate it.

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

Standards and guidelines are typically used as security frameworks by the organizations in question. They define a baseline for corporations and agencies to work off of and within while still affording the firm the ability to apply context to the framework. This helps the firm establish a known system of security controls and force it to address known or unknown risks within the organization through risk assessments and audits. They also offer a generalized approach to security through the use of various administrative, technological, and physical controls across different levels and teams within the organization. The goal of such standards and guidelines is typically to be able to implement practices such as the above in a repeatable, sustainable, cost efficient, measurable way and to allow these practices/controls to mature over time as the security system matures.

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

Most companies have methodologies and processes in place for the allocation of resources. However, generally speaking these methodologies are implicitly defined and, as such, are not subject to measurement by the maturity framework of the organization if one is in place. If an explicit methodology is defined, the maturity of it is highly dependent on the size, sector, age, and process maturity of the firm in question as well as its resource capabilities. In regards to cyber security, the typical process flow for allocation of resources would typically begin with either a strategic business initiative or a regulatory and compliance need. These requirements would facilitate the choosing of a specific technology (in the case of IT projects) or a specific framework (in the case of security) which would lead to estimates of requirements of resources in terms of employees and capital.

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

This question is similar to the last in that the answer is heavily dependent on the firm in question. The characteristics of the firm that the answer depends on are size, sector, age, process maturity, and current security posture of the organization. Firms that are under various regulations for cyber security will tend to have more resources allocated to security and will likely have processes in place to respond a highly severe security risk. However, firms whose security policies and processes are immature and who are not under heavy cyber security regulations typically do not invest in these areas and will be far less prepared or trained to react to a drastic swing in cyber security risk.

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

Actually these practices are more to protect our privacy and civil liberties. Not implementing best practices to ensure the Confidentiality, Integrity and Avaliability of our critical information enhances our ability to live and feel more secure.

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

Actually other countries such as the EU and Asia are also going down this same path. Talking the same language using standards provides an international link to ensure the rights mentioned above are protected no matter where you do business.
https://www.gov.uk/government/consultations/cyber-security-organisational-standards-call-for-evidence
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/132466/bis-13-659-cyber-security-organisational-standards-call-for-views-and-evidence.pdf

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

Every time we use a credit card, swipe a subway pass, or send an email we are sharing personal information about ourselves. Just how is the information used? How do we balance an individual's right to privacy vs. community safety?

The good news is that international standards provide a reasonable and workable solution for grappling with the problems of excessive data collection. They provide an unbiased and internationally accepted way to ensure industries are bound by same basic privacy principles to protect information and continuously monitored. In the same way, the government should enforce similar principles to ensure protection of our critical infrastructure. It is a matter of national security.

Unless the government acts quickly to rein in the unchecked collection of online data, we may end up with a complete surveillance state online – one that is not built by the US government, ironically, but by external forces (possibly other governments) mining information. Such a scenario has alarming implications for Internet users and the Internet itself, as constant tracking and surveillance chills the freedom and participation that makes the Internet the useful and important medium it is today

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

The following are the list of core practices taken from internationally accepted cyber security frameworks that we believe should be included in the framework:

- Accountability for risk management at upper layers of the organization
  - This allows the risk management responsibility to be spread across the organization and, with accountability at the upper layers, forces those with the ability to effect change to make the critical decisions.
- Personnel security training and education requirements

  - Continual personnel security training and education reinforces the fact that security risks surround all companies at all times. It also allows employees to evolve and stay abreast of the latest trends in security and their impacts on the organization.
- External audit requirements for the guidelines defined in the framework
  - External audits force companies to continually invest in their security posture and maintain controls so that they stay effective.
- Wireless network security requirements
  - The separation of business and operational systems requirements hints at protection of wireless networks but they are a special concern within environments that contain critical infrastructure and should be accounted for appropriately.
- Perimeter defense requirements
  - The separation of business and operational systems requirements hints at the defense of the network perimeter, but explicit requirements should be made regarding this important area of critical infrastructure. It should require that the internal network be explicitly separated from the Internet via standard defenses such as proper routing and firewalls.
- Automated preventative tools and capabilities
  - The incident detection tools and capabilities requirement specifies that the organization should have the ability to detect security issues. However, due to the lack of resources and manpower it vitally important that the organization have the ability to prevent attacks in an automated fashion. This can include general controls such as anti-virus, a properly configured firewall, or an intrusion prevention system.
- Establishment of an explicitly defined vulnerability management system
  - The easiest attack vector for an adversary is to exploit systems on the network that have not been patched for years. Due to the sensitive nature of their businesses most firms that support or host critical infrastructure do not have a proper vulnerability management system in place. These systems typically include policies and procedures related to continuous vulnerability assessment and remediation, penetration testing, and system security patching and update practices.

**Contributors:**

**John DiMaria; BSI Group America Inc**

**Taiye Lambo; Holistic Information Security Practitioner Institute (HISPI)**

**Ralph Johnson; Holistic Information Security Practitioner Institute (HISPI)**

**Danny Tijerina; RenewData®**

**Jordon Flynn; eFortresses, Inc**