Data Security Council of India (DSCI)
Inputs to the RFI
On

Developing a Framework to Improve Critical Infrastructure Cybersecurity

National Institute of Standards and Technology, US Department of Commerce

Submitted by

Data Security Council of India
Niryat Bhawan, Rao Tula Ram Marg, New Delhi , India
Ph +91 11 26155071
Fax +91 11 26155070
Email – info@dsci.in

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?

Cybersecurity practices should be developed keeping in mind the functional and operational requirement of protecting their critical infrastructure and building a resilience mechanism of the existing infrastructure. Further, Audit/ Compliance requirements with respect to federal/geographical, sectoral[1] or entity[2] based regulations are important consideration for an organization. Organizations, in their policies and in practice, should look towards for a process which are repeatable and provide maturity based evolution of the organizational practices. Comprehending all of these together and architecting these requirements as a cybersecurity practices is a major challenge for organizations. Some of the other challenges are that organizations:

I. Are unaware of the ramification of compromise to health of cybersecurity
II. Face challenges with respect to adequate funding - as security is generally a cost center and not a business priority
III. Don't have insignificant skills and their efforts and resources are generally misaligned. For example, major focus has always been on compliance reporting rather than focusing on actual security requirements.
IV. Don't have insufficient intrinsic and extrinsic drivers and mandates which drive organization to adopt cybers ecurity practices across critical infrastructure.
V. Don't have ability in defining Technical requirements, architectural positioning & solutioning for emerging threats to critical infrastructure.

Considering that the threat environment in which they operate is getting complex and dynamic; attackers are evolving innovative techniques. In such a scenario the ***practices and procedure that an organization adopts should be dynamic and evolving. The security requirements need to be agile***. Most of the cybersecurity frameworks fail to bring that dynamism and agility and revolve around compliance/regulatory requirements. As a result, though security of the critical infrastructure is of the prime importance, organizations divulge in so many compliance norms that they sometimes fail to achieve the real security.

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

The greatest challenge is to incorporate different requirements of different critical sectors under one framework. For example, the Financial sector security threat landscape would not have not much commonality with the threat landscape pertaining to Energy sector or Telecommunications sector. Currently:

I. There are inadequate efforts for cross-sector aggregation of security requirements. There is lack of drivers & mandate for the same
II. Attributes, parameters and elements of standards don't comprehend the dynamic threat requirements and challenges of the sectors

[1] Sectoral - Applicable for sector specific organizations e.g Hospitals follow - HIPAA for security of health records
[2] Entity – Applicable to all entities involved in particular type of transaction – e.g. GLBA for any financial transactions

III. Commonality exists, but, doesn't comprehend the dynamism and reality. For example, ISO 27001, FISMA does not reach to the granularity of cross sectors
IV. New approaches, references & framework are unable to compete with comfort zones of existing mechanism (ISO 27001)

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?

The organization's policy categorizes and classifies kinds of risks based on the nature of business, transactions, infrastructure setups, geography, compliance and regulatory requirements, etc.. These vary considerably based on the type of industry, type of business, size of organization and geographical spread. From the cybersecurity risk point of view, the emphasis apart from the one listed above is also on the availability of citizen services, public safety, resiliency, etc. and varies based on industry to industry. However, generally these policies are:

I. Directed at organizational security and tend to neglect the cyber security aspects
II. Top-down, missing granularity and are often misaligned and irrelevant to the cyber security requirements
III. Away of real threats and risks and focussed more on compliance demonstrations

The policies are sporadically reviewed after thorough discussions with all the relevant stakeholders and based on the consensus are effectively communicated to the intended recipients through appropriate channels and modes like internal /external audit mechanisms and are reviewed periodically based on the threat patterns and evolution of business needs. However, the senior management reviewing the policies generally

I. Lack oversight and are more focused on trivial issues, neglecting the core and remain reactive
II. Are not able to identify performance measurements relevant to the security requirements.

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

Typically they are converged at CISO/CSO/CRO level. Tactical mechanism for governance may also be present like Risk Management or compliance office. However, special focus on cyber security in Risk Management is rarely found.

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

Definition and assessment of risk, generally followed by categorization and classification, is preceded by study of threat matrix and related vulnerabilities that the organization is exposed to due to its operations. The cyber security risk may not be part of Risk Management exercise (*For further details refer Point 3.)* The challenges with Risk Management is that it

I. Tends to become simplified and naïve, negating complexity and security realities
II. Focuses on compliance demonstration, and misses on critical objective of protection
III. Lack approaches, techniques & competence that help comprehend complex dimensions of cyber security risk
IV. Does not have adequate competence and techniques required for a high level of risk governance

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

Cybersecurity risk management framework forms an important component of the overall organizational risk management framework, given the growing importance of ICT in an organization's operations and the ability of a Cybersecurity risk to result in unperceivable repercussions. However, integration of cyber security into ERM remain a challenge because of:

I. Compliance demonstration is of prime objectives, rather than protection
II. Lack of approaches, techniques & competence in cyber security capabilities and its integration with ERM

III. Inadequate competence and techniques required for a high level of risk governance

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

In India, Different organizations uses different standard and frameworks for example CoBIT, COSO is used for defining the overall framework, while ISO 27001 is majorly used as a high level controls framework, there are other framework such as PCI DSS which are prescriptive and focuses on key requirements with respect to Credit Card Data.

The DSCI Security Framework (DSF©) which has recently seen momentum is a discipline specific approach and allows organization to choose disciplines based on their nature of business. The framework focusses on providing strategic guidance, tactical measures and best practices for addressing real threats in its environment, without worrying about compliance to regulations. Further it provides maturity parameters which help organization to improve their practices continually and gradually. The framework help organization draw a strategic plan based on evolution of different disciplines of security, and their interdependencies, with continuous focus on protecting data. Refer Annexure 1 – DSCI Security Framework for further details.

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?

Not Applicable

Specifically with India following regulatory requirements exist for organizations relating to cybersecurity

I. IT Act – which defines the legal requirement of cybersecurity through various clauses defined under section 43 read with section 66 together. It also defines requirements for Privacy through section 43A and clauses with respect to contractual obligations in section 72
II. The Legal role of CERT-In with respect to incident response and monitoring has also been defined under the act which also defines the role of authority for Critical Information Infrastructure protection under section 70 A of the act.

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

There is a massive interdependency with respect to the critical assets for example the telecom sector provides major platforms through an internetworking backbone or mobile based services such as 3G or 4G which are utilized by different applications for providing services. Similarly, payment infrastructures provided by the Banking sector is being utilized by many sectors. From the energy sectors, the grids which provide energy to the services are developed through the use of ICT products majorily developed by IT companies Growing use of ICT has led to enablement of sector specific technology use, though their exist a certain level of convergence.

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

The provision for providing essential services while managing cybersecurity risk are designed based on the requirement of the users of the services during the disruption(which varies with different types), its criticality with respect to Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), and the current infrastructure capability associated with the services. It also takes into considerations the resource requirements based on people, process and technology. The performance goals thus should be associated with the:

I. Ability to sustain business/ match business requirements based on the type of exigency
II. Availability of critical resources
III. Timely restoration of services

IV. Desired functionality of services
V. Services to key stakeholders

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?

Not Applicable

Offshoot, multiple reporting should not be much of a challenge given that each regulatory body would have a defined mandate that delineates it from the other regulatory body and thus there would not be any duplicity of information that needs to be provided, other than few common items. However at a minimum following consideration should be given while defining the reporting requirements:

I. What will you require to report to make sharing useful?
II. What kind of clearing house function your require?
III. Need of mandate, drivers and incentives for reporting

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

International Standard Organizations such as ISO and International bodies such as UN, OECD etc. could play an important role in enforcement of cyber security standards for critical sectors although their role in conformity assessments needs to be carefully evaluated keeping in mind the sovereign rights of the nations. These bodies should work toward building an environment that fosters trust by maintaining faith in an organization's ability to have essentially implemented the standard it conforms to, and by possibly offering support in implementation and adaptation, rather than Assessment. Some of the positives and negatives of international standards are:

Positives

I. Help in comprehension and building structured thoughts
II. Provide attributes, elements and components for developing agenda
III. Help establish minimal base line control and competence
IV. Help plan, implement, measure and seek compliance

Negatives:

I. Procedural norms of international standards creates hindrances and delays in responses
II. Creates comfort zones, becomes static, while cyber security need dynamism
III. Creates culture of compliance documentations & demonstrations, attracting resources and efforts, leaving many desired tasks unaddressed

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?

The existing approaches are primarily categorized into

I. Information Security Management Standards- ISO 27001 falls into this category
II. Specifics of Security Management, such as Application Security, Infrastructure security
III. Technical standards: Encryption, Digital Signature, etc
IV. Industry standards such as HIPAA for health records
V. Transaction specific standards such as PCI-DSS for card transactions
VI. Entity specific standards such as GLBA for financial transactions
VII. Government Standards - FISMA
VIII. Sector specific standards, for example standards from NERC for energy sector

DSCI has published its approach as DSCI Security Framework (DSF). DSF gives a fresh perspective to the approaches of managing security by focusing on disciplines of security. This aligns with the evolution of the subjects, which is extending its scope to more granular and specific elements. Each discipline of security, because of its scale and complexity, warrants attention from strategic, tactical and operational perspectives. The discipline specific approach, thus, serves the purpose of making security more realistic, relevant and dynamic. Refer Annexure 1 for further details.

2. Which of these approaches apply across sectors?

Different approaches have different pros and cons while ISO 27001 is a good starting point for many organizations it fails to reach to granularity of the subjects. While, in case of specifics standards like the application security or a technical standard like the ones for encryption provides the granularity of security approaches. However, it may lead to challenges with respect to integration and cohesion requirements of other followed practices within the organizations. Although the approaches cited in the response to the above question provide different kind of benefits to critical sectors, our observations are confined to DSF only.

Discipline specific approach of DSF is based on the principles of ***visibility***, ***vigilance***, ***coverage & accuracy***, ***discipline in defense***; ***focus on strategic, tactical and operational layers.*** *It is applicable* to the critical sectors in the following way

I. Help making security program more specifics that provides attention to each of the elements that may have serious ramification to security or organization and health of cyber space
II. It helps enhance organization comprehension of complex affairs of security
III. It helps extends the scope of security to all desired elements and concentrate its effort to increased accuracy
IV. It makes organization more vigilant to evolving threats and makes it vibrant to the evolving trends of security

V. It providers guidance for understanding and dealing with strategic, tactical and operational perspectives of specifics of security, termed as disciplines of security in DSF
VI. It helps improve discipline in the defence planned for security
VII. It also provide sufficient insight into building compliance demonstration capabilities
VIII. It provides maturity criteria for each discipline. With total 170 criteria, it contributing to the maturity improvement cycle of an organization

3. Which organizations use these approaches?

DSCI Security Framework (DSF©) along with DSCI Privacy Framework (DPF©) are being followed by multiple organizations from different sectors as the practices in the frameworks do not prescribe to any control or specific technology but rather focus on strategic directions, approach and best practices that would help organization mature its practices in the long run. DSCI Security Framework is relevant for:

I. Those, which look for Improving maturity in specific disciplines of security
II. Those, which look for benchmarking security initiatives from strategic, tactical and operational perspectives
III. Critical sector, where the maturity in each of the discipline is important for overall security
IV. Organization which provide IT and IT enabled services to the critical sector
V. Solution vendors which map their products and services with the disciplines of DSF
VI. Security architects which designs the solutions requirement of the organizations
VII. Evaluators who are looking to assess critical capabilities for the purpose of high level of security

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

The contemporary approaches experience the limitations in the different categories such as:

I. **Control specific approach**: Security is becoming a matter of complexity, scalability and granularity. Relevancy of a set of controls is time dependent, and it loses it meaning in a shorter time span. Standards that promote the controls, although takes a lot of resources and efforts, becomes ineffective during the course of time
II. **Management standards**: Helps establish administrative and management mechanism for security. However, increasingly reliance on them creates unnecessary burdens, without actually delivering security on the ground
III. **Technical standards**: Addresses specific requirements of standardization of technology for better performance, interoperability and integration. These standards are critical, however, may not aid in the management and operation of security affairs

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

DSF proposes modification in the approach for security in the following way:

I. Identifies key principles for running security initiatives and articulates practices around them: ***Visibility; Vigilance; Coverage & Accuracy, Balance of Strategic, Tactical & Operational views; Discipline in Defense . & Compliance Demonstration***
II. ***Focuses on a strategic treatment to security*** that will not only mature its endeavour but also optimize the resources and efforts deployed.
III. ***Brings dynamism and agility in security operations*** because of which it Helps align security to current trends understanding & practices
IV. Helps organizations with inputs on building strategy in the 16 distinct disciplines of security which ensures comprehensiveness & coverage. It provides implementation guidance For each discipline, DSCI recommend approaches and processes that help take a strategic review of an organization's initiatives
V. Provides 170 maturity metric criteria to enhance maturity of security program
VI. DSCI focuses on a 'Visibility' exercise, which brings a consolidated view of data at the central level. It analyses and identifies the integrated view of the data within the findings. It creates a risk profile that is data centric
VII. Assigns importance to the key aspects of security capability management such as 'maintaining comprehensiveness & dynamism of organizational understanding', 'responsiveness to threats',

'aligning protection measures to the actual security threats', and 'ability to drive organizational actions for security & compliance assurances'

VIII. Concentrate on convergence, integration and collaboration to realize the objectives of security governance

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

There are specific sector security standards like the one developed by NERC for energy sector and 3GPP/3GPP2 for telecom. As they are supposed to address specifics, these developments should be welcomed. Further, any cross sector standard should not only aim to address the baseline requirements of each and every sector it ascribes to, but also have certain components (also known as Delta practices) pertaining to specific sectoral requirements that ascertains the completeness of the framework and that it could be applied to any organization irrespective of the sector the organization operates in.

An alternative approach to this can be a standard similar to DSF which focuses on specific security disciplines such as application security, Security Organization, Infrastructure security, etc.. The applicability of a particular discipline varies from organization to organization and the nature of business transaction. For example, IT industry can focus on aspects like infrastructure security if they provide infrastructure services or Application security, if they are involved in application development. This method will ensure that the cybersecurity standard is relevant to cross industry and will allow industry to choose disciplines which are relevant for their nature of businesses.

Ability of horizontal standards to address the security requirements is always challenged. DSCI Security Framework (DSF) provides unique benefits to address sector requirements as follows:

I. Discipline specific approach provides modular approach, helping to focus on those disciplines that are pertinent to a sector
II. Measurement metrics provided by DSF may be scaled and weighed to sector specific requirements

Additional sector specific modules, over and above the practices prescribed, while emphasizing on specific technologies and controls required could make them more adoptable and implementable. The approaches need to constantly update themselves, given the rapid pace of technological advancement and emerging requirements originating from specific sectors. While designing sector specific modules, thorough assessment of each sector must be carefully undertaken to understand its threat matrix, the existing vulnerabilities, and the gaps in existing policies, technology landscape, and overall requirement of the sector.

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

For specific sector it would be pertinent to have specific standards as their business ecosystem, technology profile and threat landscape may be fundamentally different from others. If there is a chance that security compromise in that sector will lead to significant impact, then it will be important to have sector specific development. Voluntary program may yield desired results if the sector is well awakened, security is priority for business and there is will and actual investment in security. The sectors may be motivated or driven to develop their own standards. However, the development of the standards, as cited in response to above questions, shouldn't lead to rigidity and lethargy.

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

Their role in designing becomes all the more important given their critical role in promoting the use of the approaches. They should be appropriately consulted at each and every stage and their inputs be sought timely to ensure consensus-based standards is developed to the fullest extent possible. Some of the sectors witness competent institutional development, either in the form of regulator or industry forum. They play crucial role of driving the initiatives in the sector. However, while relying on these institutions a

care must be taken that they possess adequate skills, competence, resources and empowerment to drive security.

9. What other outreach efforts would be helpful?

The focus of the outreach efforts should be to

I. Educate and make the sectors aware of cyber security issues
II. Do an In-depth analysis of critical security issues that may lead to huge and kinetic impact
III. Enhance the cooperation and collaboration within the security community
IV. Share information on security incidents, attack vectors and exploitations
V. Drive the coordinated programs and initiatives
VI. Enhance skills and competence

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?

Most of the above listed practices are widely used throughout the critical infrastructure and industry primarily as per the business need and may not be from the concerns of national cyber security. The state and maturity of the practices may be varied, which may not deliver consistent security performance across the companies and sectors. Each of the above practices requires organizational capabilities to ensure the desired level of governance. Some organizations may have better access to those capabilities than others. Removing this disparity through different policy means may be one of the objectives of the framework being discussed here.

Some of the above practices are also devised in the form of different disciplines as defined in the DSF. The practices provides a strategic guidance to the organizations, it discusses the approaches, trends and practices that are driving an individual discipline and finally provides a detailed guidance for systematically planning and implementing security in the organization..

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

These practices form the core of any standard that advocates comprehensiveness. While designing any policy framework, such critical aspects must be given due importance. However, Some of the practices such as ‘Security Engineering’ , ‘Monitoring and detection tools and capabilities’ and ‘Privacy and civil liberties protection’ may not be seen quite frequent in the existing international standards and practices

DSCI security framework (DSF) together with DSCI Privacy Framework (DPF) addresses these requirement however it does not specify any controls. Instead, it outlines best practices in these disciplines that are based on recent learning by organizations, analysts, and technology and solution providers. It leaves to the organization to select and implement controls specific to its operating environment and business requirements. DSCI focuses on a ‘Visibility’ exercise, which brings a consolidated view of data at the central level. It analyses and identifies the integrated view of the data within the findings. It creates a risk profile that is data centric. DSCI makes uses of its Best Practices approach to evaluate strategic options, both in terms of the processes and technological solutions available for addressing these risks, and strengthening the security posture. DSCI believes that once visibility over data is created at the central level, it is easier to bring dynamism in the security program as recent trends, vulnerabilities and incidents can be considered and appropriate risk management measures can be taken on a continuous basis.

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

All the listed practices are critical and their criticality differs from sector to sector. A practice might be highly significant in one sector while in some other sector, its criticality may reduce. However, following looks more relevant for secure operation of critical infrastructure

I. Separation of business from operational systems;
II. Use of encryption and key management;
III. Identification and authorization of users accessing systems;
IV. Incident handling policies and procedures;
V. Mission/system resiliency practices

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

Depending on sector to sector, some of the practices listed above might not directly align with business or mission needs of an organizations, However all these practices looks relevant for all the sectors

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

I. Security engineering practices and Privacy and civil liberties protection are most difficult to implement given that they have to be factored in at each and every stage in the design and implementation phase in the information life cycle.
II. Incident handling tools and capabilities because of the increasing complexity, innovative &targeted attacks, and inability to comprehend rules to identify those attack patterns

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

It is always beneficial to understand how these practices are designed, implemented and followed by other organizations that have already adopted them. The study of existing implementation helps identify gaps and loopholes while providing organizations an opportunity to plug them while designing and implementing their practices.

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

Being industry initiative, and author of security framework, DSCI assigns significant efforts and resources in acquiring knowledge, analysing operating scenarios and distil policy and strategic initiatives. It also significantly invest in tracking and studying technology evolution, trends and practices

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

Most of the organizations these days follow a well defined escalation matrix that is significantly matured and has provision to address cyber security risk even with a sudden increase in severity. However, it would be matter of detailed study to see if the existing escalation process address cyber security.

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

The greatest and foremost risk is the fear of violation of any regulation/ law/ practice that prescribes Privacy protection and guarantees civil liberties to the individuals as an entity and the society at large.

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

This framework, if properly designed and implemented, might play a very crucial role in global arena given its reach on the businesses and related policymaking and standards development by other bodies and countries.

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

These risks demands a comprehensive as well as careful study of all the related aspects of privacy and civil liberties that are applicable to an organization and should be notably considered by the organization while designing and implementing any framework.

DSCI Privacy Framework boasts of a robust architecture that helps an organization mature its overall competence and capability of privacy and mature its practices that guarantee privacy protection to the individuals. Please refer DPF© for more details.

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

In addition to the practices noted above, following practices may also be considered for inclusion:

I. Threat and Vulnerability Management – refer TVM in DSCI Security Framework
II. Security Audits, Testing and Compliance – refer SAT in DSCI Security Framework
III. Having a developed security organization – refer SEO in DSCI Security Framework
IV. Third party security Management – Refer TSM in DSCI Security Framework
V. Special focus on Data/Information security – Refer DSC in DSCI Security Framework

Annexure 1 DSCI Security Framework

Many organizations worldwide have adopted widely accepted & internationally recognized security frameworks and standards such as ISO 27001, which provide guidance & direction for establishing enterprise wide security processes and procedures. But problem arises when organizations channelize investments and resources to demonstrate compliance to such standards (e.g. extensive documentation, huge checklists) instead of identifying and mitigating real risks. Similar has been the case with FISMA implementation in the United States –compliance to it has taken precedence over real security in the networks and systems of the federal agencies.

Organizations today need to be 'really' secure, as the threat environment in which they operate is getting complex and dynamic; attackers are evolving innovative techniques. In such a scenario, organizations cannot rely on certifications alone, even though they may help provide assurance to their stakeholders. Though ISO 27001 standard, is a good starting point for organizations for implementing security, it is not an end by itself. When organizations operate in a vibrant, dynamic, evolving and competent environment – be it business, regulatory or threat environment as in case of security, organizations can only survive if they are able to draw a roadmap for coming years that entails future conditions & requirements, strategic options, building required competencies, etc. and not just focus on the present. This is achieved by doing long term planning and drawing a strategy to achieve the defined goals. But how many organizations today have a security strategy? How many organizations have a 5 year vision for security? Unfortunately - not many. Though, ISO 27001 has been phenomenal in establishing enterprise wide security processes, it falls short in the following areas:

1. ***Long Term Strategic Planning in Security*** –Today, security practitioners strongly believe that security should be treated as a business enabler and not as a hurdle – adding value to business, by allowing business to offer innovative solutions & services to international markets round the clock, increasing productivity, reducing cost, providing customer delight, etc. If such an approach needs to materialize, security needs to be revitalized by working more closely with the business and IT and being given strategic importance within the organization. Unfortunately, many standards are controls based standard - controls that are static in nature, focused on mitigating the existing risks, not focused on addressing the futuristic requirements / risks that emerge from business expansion and innovation.

2. ***Building Security Capability / Competence, using Maturity Criteria*** - Security is a continuous journey, and no organization can be 100% secure. However, it is important to measure the progress made / capabilities built over a period of time to address the evolving and perennial threats. This can be achieved by defining criteria against which an organization can measure its capability maturity in security. Many standard on the other hand promotes a 'yes/no' kind of approach to security, wherein an organization is certified as fully compliant if it has implemented the relevant controls. It does not provide any maturity criteria, which organizations can leverage to improve their security competence.

3. ***Focus on Protecting Data*** – Many standards follow an asset centric and process oriented standard. Processes help provide guidelines for conducting operational tasks in a pre-defined manner, but if too much focus is given on processes, then it may happen that the objective for deploying a particular process may get lost (outcome may not be achieved). This also at times results in loss of productivity and is perceived as bureaucratic. In today's digital world, data has an economic value attached to it. In fact, in some industries like pharmaceutical, data is the life line of the organizations operating in the sector. Hackers and rogue insiders vie for this critical data. In such a scenario, the focus of all the security efforts should be on data, with lean processes and intelligent technologies deployed to protect it..

4. ***Tracking Security Evolution*** – Security as a discipline has evolved over a period of time. The stimuli have been many - the dynamic threat landscape, strengthening regulatory regime, research & innovation, globalization, business models, technologies, etc. For an organization to be secure it is important that it keeps track of all the latest developments taking place in the field of security – be it

skills, technologies or services. Today, specific security disciplines have evolved with very specific approaches to address the unique challenges faced. Specific trends and practices have been emerging to address the exact requirements of an individual discipline. The security market, both technology products and services, has solution offerings specific to an individual discipline. Security profession is also charting a path of specialization in these individual security disciplines. For e.g. Management of threats & vulnerabilities is a very critical discipline today, requiring specific skills, technologies and practices. Similarly, disciplines like Secure Content Management, Governance, Risk & Compliance do not find their rightful place in ISO 27001 standard. It fails to provide strategic and contemporary directions and guidance to organizations that are implementing and maintaining security.

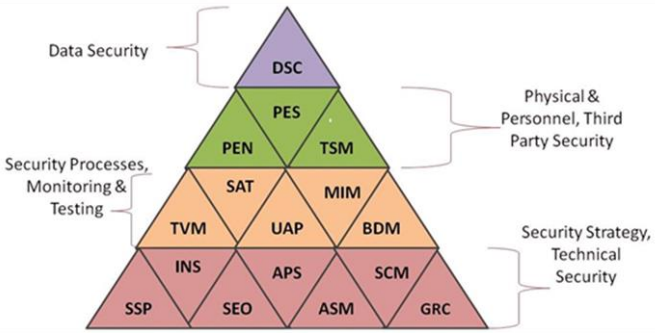
5. ***Integration and Interdependencies –*** Security disciplines, as explained in the point above, have number of interdependencies and therefore there is need for taking an integrated approach that links these disciplines appropriately for better protection. For e.g. Security Incident Management as a discipline requires inputs from Threat & Vulnerability Management, Infrastructure Management, Application Development, etc to be effective. ISO 27001 standard does not take such an integrative approach as it is focused on individual controls that are described and deployed in silos.

There is a need to approach security differently - a way that helps overcome the above shortcomings of ISO 27001 and enables an organization focus on real threats in its environment, without worrying about compliance to regulations. It should be able to assess organization's maturity in implementing security in different areas with a view to continually improve the same. Such an assessment should further help organization draw a strategic plan based on evolution of different disciplines of security, and their interdependencies, with continuous focus on protecting data. Compliance should be the outcome along with dynamic and vibrant security that enables quick response to threats, vulnerabilities and actual cyber-attacks.

DSCI Security Framework (DSF©) achieves precisely this. **It is based on the following three foundational elements**:

a. ***Security Principles***: Starting point of DSF© is a set of security principles that an organization should seek to adhere to. These include information ***visibility***, ***vigilance***, ***coverage & accuracy***, ***discipline in defense***; ***focus on strategic, tactical and operational layers and compliance demonstration***. DSCI believes that approach to security which is based on these principles helps remove the focus from extensive documentation, checklists and controls, and enables an organization achieve dynamism in security which gives it the agility to respond to threats and attacks.

b. ***Discipline Specific Approach***: DSF© view of security is ***discipline-specific***. Unlike other standards, it does not specify any controls. Instead, it outlines best practices in these disciplines that are based on recent learnings by organizations, analysts, technology and solution providers. It leaves to the organization to select and implement controls specific to its operating environment and business requirements. It identifies maturity criteria in each of the 16 disciplines that form part of DSF©. While these disciplines are organized in four layers, it encourages organizations to focus on each individual discipline of security by implementing best practices, and moving up in maturity rating by using the maturity criteria. Focus on individual disciplines, and striving to achieve excellence in them is the path to real security.



c. ***Data-Centric Methodology***. DSCI focuses on a 'Visibility' exercise, which brings a consolidated view of data at the central level. It analyses and identifies the integrated view of the data within the findings. It creates a risk profile that is data centric. DSCI makes uses of its Best Practices approach to evaluate strategic options, both in terms of the processes and technological solutions available for addressing these risks, and strengthening the security posture. DSCI believes that once visibility over data is created at the central level, it is easier to bring dynamism in the security program as recent trends, vulnerabilities and incidents can be considered and appropriate risk management measures can be taken on a continuous basis.

Corollary to the visibility exercise is the establishment of privacy initiatives in the organization, since the flow of personal information processed reveals exposure to privacy risks at various stages. The DSCI Privacy Framework (DPF©), which has identified nine privacy principles for achieving privacy in an organization, through the implementation of nine best practices which are organized in three layers – Privacy Strategy & Processes, Information Usage, Access, Monitoring &Training and Personal Information Security for establishing privacy initiatives in an organization, helps an organization do that.

Practices in each discipline of DSF© have been articulated under the following four sections:

- ***Approach to the Security Discipline***: DSCI believes that there is a significant requirement of discussing the approaches, trends and practices that are driving an individual discipline. This section in each discipline articulates DSCI approach towards the discipline under discussion.
- ***Strategy for the Security Discipline***: DSCI also believes that each security discipline deserves a strategic treatment that will not only mature its endeavour but also optimize the resources and efforts deployed. For each discipline, DSCI recommend approaches and processes that help take a strategic review of an organization's initiatives. This section will help managers to provide a strategic direction to the organization's initiatives in each discipline.
- ***Best Practices for the Security Discipline***: DSCI recognizes a need for providing a detailed guidance for systematically planning and implementing security in the organisation. This section, in each discipline, compiles the best practices for the security implementer.
- ***Maturity of the Security Discipline***: DSCI believes in assessment of the outcomes and for fair assessment, comprehension of appropriate parameters is necessary. The DSF© has defined a total of *170 maturity criteria* for the 16 disciplines.

DSF© especially through its maturity criteria can be used to determine an organization's security capability in different disciplines of security. This can be of particular relevance in outsourcing relationships where client organizations want to determine the overall and / or Line of Service specific security capability of service provider organizations.

Framework Benefits

DSF© offers key benefits as follows:

Offers a set of principles for implementation of true security	*Helps align security to current trends understanding & practices*	*Focuses on bringing relevance to security, hence, realistic security*
Provides means to improve dynamism in security	*Ensures comprehensiveness & coverage through the disciplines*	*Provides strategic directions to security initiatives*
Offers detailed guidance for implementation	*Supports maturity improvement through outcome based metrics*	*Promises revitalization of security initiatives for data security*
Provides means for integration, convergence & collaboration	*Content support to manager, implementer, consultant, auditor*	*Comprehensive and structured ecosystem around the framework*

For more details on DSF© visit: http://www.dsci.in/dsci-security-framework

For more details on DPF© visit: http://www.dsci.in/dsci-privacy-framework

DATA SECURITY COUNCIL OF INDIA

A NASSCOM® Initiative

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India
P: +91-11-26155071 | F: +91-11-26155070 | E: info@dsci.in | W: www.dsci.in