Appendix U

DSCI Security Framework (DSF) from Data Security Council of India

Introduction

We are in the era of digital economy wherein critical information assets reside on corporate networks. One cannot perceive global business delivery without the underlying IT infrastructure to support organizations. Data Security Framework (DSF) is one such framework that has emerged from India and it has the potential to become a global standard soon. Our readers ought to know about this framework and therefore it is introduced in this appendix. The entire gamut of Information Systems Security is available in *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* by Nina Godbole.

The foreword of the book vividly describes the current scenario in India along with the global perspective. Chapter 1 provides an overview of cybercrimes and in Chapter 9, it is explained as to how organizations need to be alert to protect themselves from a range of possible avenues for cyberattacks in the modern world. In the current paradigm, it is crucial for organizations to take reasonable precautions for safeguarding their information assets and confidential business information. When suitable controls are established, it becomes important to have those controls and related best practices evaluated. When assessment or evaluation is done, it is always with reference to a framework. From that perspective, this appendix introduces the data security framework that, as mentioned before, has emerged from India.

DSCI and DSF

DSF© is DSCI Security Framework developed by *Data Security Council of India* (DSCI). DSCI, operating under the aegis of NASSCOM, is a self-regulatory initiative in (a) *data security* and (b) *privacy protection*. It is envisaged as a credible and committed body to uphold a high-level of data privacy and security standards.

DSCI Security Framework brings a fresh outlook to the security initiatives of an organization by focusing on each individual discipline of security. Each security discipline, as depicted in DSF© (refer to Fig. U.1) has evolved with very specific approaches to address the specific challenges faced by it.

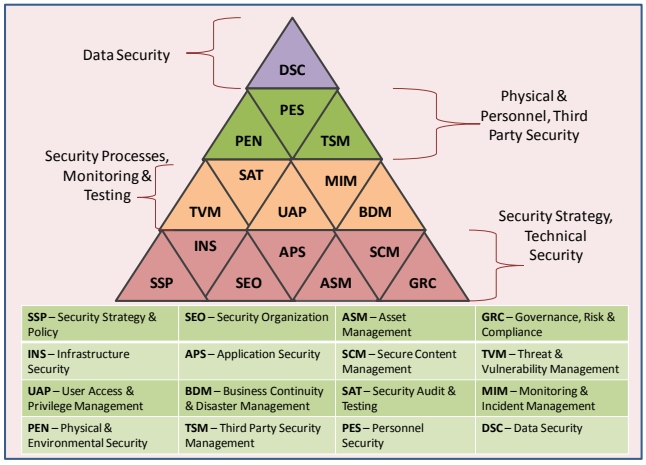

Figure U.1 The DSCI security framework.

Specific trends and practices have been emerging to address the specific requirements of an individual discipline. The security market, both technology products and services, has solution offerings specific to an individual discipline. Security profession is charting a path of specialization in these individual security disciplines. DSCI believes that the time has come for an organization to focus on individual disciplines and strive to achieve excellence in it. Thus, as mentioned before, DSF© has all 16 disciplines and was released during the annual security summit held in December 2010.

Structure of the DSCI Security Framework (DSF)

As mentioned before, DSCI Security Framework (DSF©) is a formation of *16 disciplines* or areas that are organized in *four layers* (refer to Fig. U.1). DSF© presents a specific structure for articulating its practices under each of these disciplines. The structure divides the content of each discipline into four sections:

1. **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 of each discipline articulates DSCI approach toward the discipline under discussion.
2. **Strategy for the security discipline:** DSCI also believes that each security discipline deserves a strategic treatment that will not only mature its endeavor 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 initiative. This section will help managers to provide a strategic direction to the organization's initiatives in each discipline.
3. **Best practices for the security discipline:** DSCI recognizes a need for providing a detailed guidance for systematically planning and implementing security in the organization. Under each discipline, this section, throughout the DSF©, compiles the best practices for the security implementer.
4. **Maturity of the security discipline:** DSCI believes in assessment of the outcomes and for fair assessment comprehension of appropriate parameters is an obligation. DSF© has defined the maturity criteria for each of the discipline under this section.

How the Framework Adds Value to Organizations

The DSF© framework comprehensively covers all aspects of organization's security requirements; it does that by providing a discipline-specific approach to security. The security best practices are organized in *16 disciplines* as follows*:*

1. Security Strategy and Policy (SSP).
2. Security Organization (SEO).
3. Asset Management (ASM).
4. Governance, Risk and Compliance (GRC).
5. Infrastructure Security (INS).
6. Application Security (APS).
7. Secure Content Management (SCM).
8. Threat and Vulnerability Management (TVM).
9. User Access and Privilege Management (UAP).
10. Business Continuity and Disaster Management (BDM).
11. Security Audit and Testing (SAT).
12. Security Monitoring and Incident Management (MIM).
13. Third-Party Security Management (TSM).
14. Physical and Environmental Security (PES).
15. Personnel Security (PEN).
16. Data Security (DSC).

The best practices for each of the discipline areas are specified in the full document of DSF© framework. The DSF© framework not only aligns well with the clauses of the ISO 27001 (see Fig. U.2) but it also adds value by providing parameters for "maturity criteria" for assessing each discipline listed earlier. The maturity criteria parameters are presented in Table U.1.

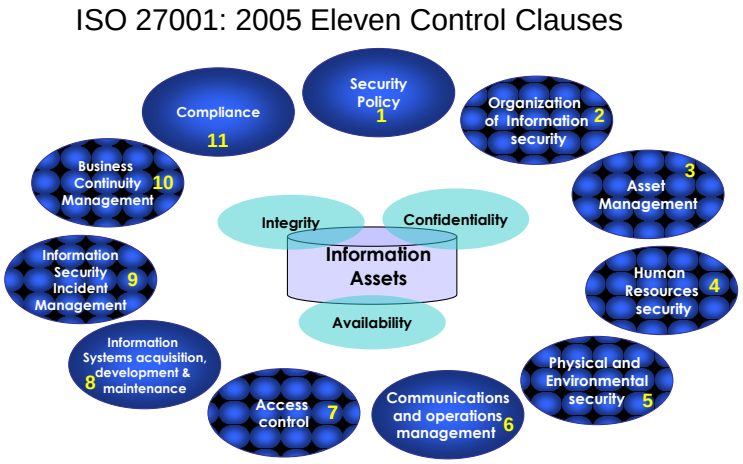

Figure U.2 The clauses in ISO 27001: 2005 11 control clauses.

Table U.1 Discipline area-wise maturity criteria in Data Security Framework

Discipline Acronym	***Name of the Security Discipline***	***Parameters for Maturity Criteria***
1. SEO	Security Organization	• Visibility over the activities, functions and operations that are attributed to security or considered significant from security perspective. • Distribution of security function at the organizational units and layers. • Strategic positioning of the security organization. • Elevation of CISO's responsibilities and skills. • Alignment of security function with business objectives. • Clarity in roles and responsibilities (of security staff/security team). • Balancing of operational tasks between IT and IT security. • Level of collaboration among various functions in the organization. • Adequacy of skills and resources. • Proportion of skills distribution commensurate with the requirements and challenges at hand.
2. APS	Application Security	• Comprehensiveness and accuracy of coverage. • Visibility over application security activities. • Adequacy of protection. • Intelligence over application security information. • Architectural treatment to application security. • Alignment with overall security strategy. • Integration with SDLC process. • Tools and technology direction. • Involvement of ADM function. • Adequacy of resources and skills. • Responsiveness to threats. • Compliance demonstration.
3. TVM	Threat and Vulnerability Management	• Complete visibility over the IT infrastructure components.

		• Homogeneity and standardization of the IT infrastructure. • Coverage of the TVM program. • Architectural treatment to the TVM solution elements. • Completeness and accuracy of the measures. • Enforcement of technical policies. • Configuration and Change Management Maturity. • Responsiveness to new security issues. • Integration with IT infrastructure management process. • Operational excellence.
4. MIM	Security Monitoring and Incident Management	• Visibility into logs and incident management process. • Coverage of the incident management program. • Architectural treatment to MIM. • Information collection capability. • Extent and accuracy of security monitoring. • Intelligence over security information. • Responsiveness to incidents. • Adequacy of resources and skills. • Amalgamation with remediation processes. • Involvement of operating groups. • Compliance demonstration. • Employee awareness.
5. BDM	Business Continuity and Disaster Management	• Complete visibility into BDM readiness. • Alignment with business requirements and involvement of business management. • Shift from tactical level to strategic vision. • Focus on integrating silos of operations. • Proactive approach and focus on prevention. • Availability architecture initiative. • End-to-end service continuity. • Scenario-based planning. • Continuity plan documented and actionable. • Systematic recovery – Recovery Services Catalog. • Focus on critical gap closure. • Comprehensive resiliency testing. • Operational practice rather than a project-based approach. • Operational excellence.
6. SAT	Security Audit and Testing	• Business alignment of investments into security and testing. • Ability to serve enterprise risk management. • Standardization of audit and testing processes. • Ability to identify critical issues and invoke a response to identified issues. • Coverage and accuracy of security audit and testing processes. • Responsiveness in testing relevance of new issues in organization's environment. • Knowledge management – testing and audit information management. • Organizational understanding of security concepts, issues, threats and vulnerabilities. • Adequacy of skills and technical competence. • Optimization of resources and efforts for audit and testing. • Integration with IT infrastructure management process for timely remediation.

7. TSM	Third-Party Security Management	• Portfolio of business services from security perspective. • Visibility into data, data environment, data access and operations in each sourcing relationship. • Integration of security in vendor life cycle processes. • Integration of vendor security operations with enterprise security management processes. • Coverage of TSM program.
8. PES	Physical and Environmental Security	• Visibility into PEN functions. • Proportionality of countermeasures. • Standardization of approaches and processes. • Technical directions. • Convergence of physical and logical security. • Integration and collaboration with other security initiatives, departments and functions. • Capacity and performance management of environmental security system. • Awareness across organization.
9. PEN	Personnel Security	• Coverage and accuracy of background checks. • Involvement of HR function. • Integration of security with HR processes. • Ease of access to security policies. • Coverage and adequacy of training and awareness. • Adequacy of administrative rules and procedures. • Enforcement of Acceptable Use Policy. • Responsiveness to non-compliance issues.

DSCI Contact Details for Further Information and Implementation Guidance

The full document for the DSF is available with Data Security Council of India. Organizations interested in implementing the framework can contact Director – Data Protection at DSCI – the details are provided below:

Director – Data Protection
DATA SECURITY COUNCIL OF INDIA (DSCI) | A NASSCOM® Initiative
L: Niryat Bhawan, 3rd Floor | Rao Tula Ram Marg | New Delhi 110057, India
P: +91-11-26155071 | F: +91-11-26155070 | M: +91-9873083123 | E: info@dsci.in
Website: www.dsci.in

Further Reading

Additional Useful Web References

1. Read article *India's Security Environment* at: http://www.nasscom.in/upload/10157/10%20india'ssecurity.pdf (18 December 2010).
2. A presentation on *Data Protection and Security: Legal Frameworks* is available at: http://persmin.gov.in/writereaddata/AnnexureB-123.ppt (16 December 2010).

Books

1. Godbole, N. (2000) *Information Systems Security: Security Management, Metrics, Framework and Best Practices*, Wiley India, New Delhi. Refer to Chapter 35 (Auditing for Security).
2. Ibid, Chapter 7 (Overview of Physical Security for Information Systems).
3. Ibid, Chapter 11 (Network Security in Perspective).
4. Ibid, Chapter 22 (Security Models, Frameworks, Standards and Methodologies).
5. Ibid, Chapter 23 (ISO 17799/ISO 27001).