7-2004

INFOSeMM: Infosys IT Security Maturity Model: A Report

Arcot Desai NARASIMHALU
Singapore Management University, desai@smu.edu.sg

N. Dayasindhu
Infosys Technologies Ltd.

Raghavan Subramanian
Infosys Technologies Ltd.

Citation

Narasimhalu, Arcot Desai; N. Dayasindhu and Raghavan Subramanian. 2010. *INFOSeMM: Infosys IT Security Maturity Model: A Report*. Singapore: Singapore Management University.

INFOSeMM: Infosys IT Security Maturity Model

A report arising from the summer 2004 visit of

Arcot Desai Narasimhalu
Practice Associate Professor,
Deputy Director, Research Institute,
Director, Industry Relations,
School of Information Systems,
Singapore Management University

21 July 2004

Alphabetical list of contributors

N. Dayasindhu
Arcot Desai Narasimhalu
Raghavan Subramanian

INFOSeMM: Infosys IT Security Maturity Model 1

Acknowledgements and Recommendations 3

1. Executive Summary 6

2. The Business Problem 7

3. The Challenge 10

4. The Solution 17

4.1. The model 17

4.2. Threats 21

4.3. Domain / Vertical Dependence 23

4.4. Expected benefits from IT Security investments 24

4.5. IT Security Maturity Levels 26

5. The Transition. 33

5.1. Considerations for developing questionnaires to assess maturity index. 40

5.1.2. Considerations for generating the questionnaires for assessing the maturity index for the intelligence pillar. 46

5.1.3. Considerations for generating the questionnaires for assessing the maturity index for the Practices pillar. 50

5.1.4.Methodology for deriving INFOSeMM maturity ratings. 56

5.2. Transition plans. 59

6. Business opportunities for Infosys 79

7. The road ahead 92

OCTAVE 94

Acknowledgements and Recommendations

The team acknowledges the support provided by the Infosys SET Labs management for initiating this work. This work was accomplished within a short period of six weeks. It should be treated as a starting framework that needs to be fine tuned through pilot studies and deployment. The tables containing considerations for questionnaires assembled form a starter kit and should be maintained for their completeness and correctness by the Infosys' client facing consultants. The mandatory maturity levels reflected in the last column of the questionnaires should also be maintained by designated consultants. The transition plans should always remain in synch with the questionnaires.

We also acknowledge the enthusiastic inputs and discussions with the following groups:

- Progeon
- BCM
- DCG
- BOFA

Their inputs and recommendations were vital for shaping this work.

List of reviewers

Date	Names	Unit	Major observations
6 July 2004 12:30 – 1:30 pm, Sarojini Naidu, B19	Ravi Raman and Nirmal Rajaram	Progeon	1. The framework will be very useful to Progeon to increase its business. 2. It is more appropriate to rename the levels from 0 to 3. 3. A tool that will help companies do self-assessment of their maturity index would be useful. 4. Progeon has generally been focused on People and Process. This framework uses eight vulnerabilities and hence is quite comprehensive and we particularly like the abstraction into infrastructure, intelligences and practices. 5. Addressing accountability is very appropriate. 6. Different verticals and even different applications within a single company may need to operate at different maturity levels. It is best for client facing consultants to decide on the levels at which a company or application is to operate.
B21 20th July 3 – 4:30 pm	Jamuna Ravi and a team of 15 others	BCM	1. Need to be clear about whether different industries need to operate at different levels of maturity. 2. How does this map into BS 7799 or OCC? 3. Can there be a single number for the rating as opposed to the present three digits. 4. Should pilot within Infosys before OCC team comes in September. 5. Will give a contact for the OCC team.

B19 21st July 21, 2004 2:00 – 3:15 pm	M.P. Ranganatha Kannan Amaresh	DCG	1. This is aligned with Basel 2. 2. This can be positioned as a dash board for the executive management team. 3. DCG banking group will work with SET Labs on this. 4. Would like to receive a single slide to run by clients. 5. Should work with Malya to see how we can apply this to Infosys. He may have three or four clients sitting in front of him who could benefit from this. 6. Will want to publish the results in domain oriented journals. 7. Will address several queries from clients. 8. Clarity on whether this IT Security maturity or Information maturity will help. 9. DCG will start with banking and will then pilot this in other groups.

1. Executive Summary

Infosys IT security Maturity Model (INFOSeMM) has been developed with the objective of assessing an organization's level of preparedness in handling cyber threats. We use the phrase IT security to also mean Information Security.

Infosys is currently perceived as an information technology service provider. The ISM model can move Infosys up the value chain by opening up a significantly increased revenue stream to the higher margin IT security consulting and let such consulting assignments lead to new IT security assessment, design and development business opportunities. This can be grown to be an independent business unit within Infosys.

ISM is defined to be a four level model which categorizes an organization into inactive, reactive, streamlined and proactive with respect to its current status based on a study of the IT security gap analysis.

Each organization can be assigned a three letter IT security Maturity index that starts with the poorest rating of DDD to the most desirable rating of AAA.

The ratings have two purposes.

The first purpose is for the Chief Security Officer (CSO) of a company to assess and report the company's IT security maturity level to its top management. The CSO could then use the index to discuss with the company's top management the maturity level and as a result the index at which the company should be positioned. This helps the CSO to obtain IT investments commensurate with the desired positioning of the company as decided by its top management.

The second purpose is for a company to use this index as a competitive advantage in getting outsourced projects. The company's with a better index can both assure the outsourcer about their quality of service with respect to information security preparedness and as a result seek a premium for its services in comparison with its competitors.

The framework developed allows Infosys engage in three main type of assessment and resulting mitigation related projects. The three main categories are IT Security Maturity assessment, Regulation compliance and Vulnerability and threat assessment and mitigation. The Vulnerability and threat assessment and mitigation can be further subdivided into twenty four small scale assignments in order to provide for those customers who would like to take small steps towards reaching their desired IT security maturity.

Details of the IT security maturity model and the ensuing business opportunities for Infosys can be found in the following pages of the report.

2. The Business Problem

Businesses are faced with a continuing battle related to cyber security related issues ranging from cyber attacks all the way to cyber (information) war. These issues affect result in information, system, reputation, and revenue related risks. These risks arise because of vulnerabilities introduced in three major parts of the enterprise – infrastructure, intelligence and practices. Infrastructure includes network, systems and environment. Intelligence includes applications and data. Practice includes people, processes and management.

External threats constantly hope to exploit the vulnerabilities offered by an enterprise. The industry vertical or domain that a company operates in determined the extent to which it is exposed to risks as a result of the combination of vulnerabilities and threats. The risks lead to loss of current and future business (revenues), regulatory wrath, waste of precious management resources, and business costs. These are collectively termed Impact on business. A company has to respond to and manage the impact on its business due to the risks.

The following diagram captures the relationship between vulnerabilities, threats, risks, business impact and business response / action.

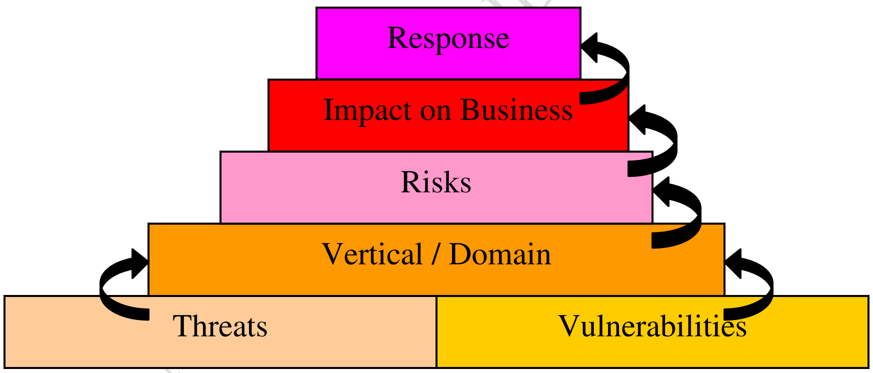

Figure 1: Relationship between threats, vulnerabilities, verticals, risks and impact on business.

Every business' executive team has no problem relating and responding to credit and other ratings issued by the likes of S&P and Moody's Morningstar stock grades. These ratings reflect the state of a business' health and hence the investment value of their companies as perceived by analysts. Executive teams in businesses do not have a means of identifying how well prepared their enterprise is, in the forecasting, identifying and managing cyber security related issues[1]. Executive teams will greatly benefit by knowing the state of their cyber security health. Once they know the state of cyber security health

[1] **Security ROI calculations pose challenges for users – November 2001**
Business-oriented approach recommended, but meaningful measurements can be elusive
By JAIKUMAR VIJAYAN
Waltham, Mass.

Information technology managers who are looking to justify their security spending would be better off presenting the issue as a fundamental business problem instead of as a technical one, according to security analysts who spoke at a seminar here last month. The business-oriented approach offers a way to demonstrate achievable returns on security investments and lets companies plan their security spending more strategically, the analysts said.

But the problem, according to users, is that there aren't many obvious ways to measure the ROI of security efforts. "We have talked about how we're going to measure ROI with the finance people, and we haven't come up with any good measures yet," said Matt Kesner, chief technology officer at Fenwick & West LLP, a law firm in Palo Alto, Calif.

Fenwick & West learned the value of tightening IT security firsthand after its Web site was taken down by a virus earlier this year. The firm plans to increase its security spending by 100% next year and has also budgeted for regular audits of its security capabilities, Kesner said. "There's a realization for the first time that security has a direct bearing on the business," he added.

In most cases, security spending usually rises only after major incidents, according to a survey released in March by IDC in Framingham, Mass. The toughest part about justifying investments is trying to assign a dollar value to the level of security needed to keep a company safe, said an IT manager at a major New York-based financial services firm who asked not to be named.

Pulling Numbers From Thin Air

"The major problem right now is that we don't have a good feel for what the real risks are and the costs [that are] associated with these risks—so that any numbers we plug into [ROI] models would be pulled from thin air," he said. One way around that problem is to stop viewing IT security as something that simply involves plugging holes, installing firewalls and reacting to the latest viruses, said Chris Wysopal, an analyst at Cambridge, Mass.-based @Stake Inc., which organized the seminar along with Bedford, Mass.-based RSA Security Inc.

Instead, Wysopal said, security should be presented as a central business issue that needs to be addressed at the start of IT projects. Potential cost savings from that approach can be used to demonstrate ROI, Wysopal added. For example, @Stake's research shows that companies that focus on security issues during the project design stage typically spend 60 to 100 times less than businesses that try to fix problems during later implementation phases or after a system has gone into use.

Sean Nolan, CIO at online retailer Drugstore.com Inc. in Bellevue, Wash., said security-related investments should be looked at more as a cost of doing business than in terms of the ROI they can generate. But no matter how security is viewed, "I think it's clear that focusing [on it] early is going to be far cheaper than the alternative," Nolan said. Putting that idea into practice, Drugstore.com has developed reusable procedures and code libraries for building security features into its systems right at the design stage, he said.

of their company, they can then decide the desired state of health and generate a plan of getting there.

All attempts have so far focused on technical aspects of information security and have not linked the vulnerabilities to exposure to risk and the resulting impact on business performance. We have developed an IT security maturity model and a corresponding index. The index can be used as a means of empowering business executives to make informed decisions on managing the business impacts of cyber security generated risks of their companies at a desired level.

Potential benefit to Infosys

The proposed maturity model can be used to position Infosys as a leader in the information security consulting business. Such consulting projects can lead to follow-on IT services projects because of the client's trust in Infosys to be Information Security sensitive in delivering their solutions. This applies to Infosys subsidiaries such as Progeon.

The maturity model can also be used as an investment by Infosys in building and maintaining customer relationships. For example, this will be a valuable tool for the Chief Security Officers or Chief Information Officers of businesses to justify their requests for investments into IT security solutions for a desired maturity level. The CSOs and CIOs are likely to be satisfied customers of Infosys.

3. The Challenge

There have been several information security related models. Three of the more prominent ones are the SSE-CMM[2] and OCTAVE[3] by Carnegie Mellon's Software Engineering Institute and CDSA[4] by the Open Group. For those dealing with US

[2] **The Systems Security Engineering Capability Maturity Model (SSE-CMM)**

The SSE-CMM describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The model is intended to be used as a:

- Tool for engineering organizations to evaluate security engineering practices and define improvements to them.
- Standard mechanism for customers to evaluate a provider's security engineering capability.
- Basis for security engineering evaluation organization (e.g., system certifiers and product evaluators) to establish organization capability-based confidences (as an ingredient to system or project security assurance).

The SSE-CMM addresses security engineering activities that span the entire trusted product or secure system life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning.

The SSE-CMM applies secure product developers, secure system developers and integrators, and organizations that provide security services and security engineering. The SSE-CMM applies to all types and sizes of security engineering organizations, such a commercial, government, and academic.

----

[3] The Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) is a framework for identifying and managing information security risks. It defines a comprehensive evaluation method that allows an organization to identify the information assets that are important to the mission of the organization, the threats to those assets, and the vulnerabilities that may expose those assets to the threats. By putting together the information assets, threats, and vulnerabilities, the organization can begin to understand what information is at risk. With this understanding, the organization can design and implement a protection strategy to reduce the overall risk exposure of its information assets. A description about OCTAVE from SEI website is attached later.

----

[4] The ***Common Data Security Architecture (CDSA)*** is a set of layered security services and cryptographic framework that provide an infrastructure for creating cross-platform, interoperable, security-enabled applications for client-server environments. CDSA covers all the essential components of security capability, to equip applications for electronic commerce and other business applications with security services that provide facilities for cryptography, certificate management, trust policy management, and key recovery.

CDSAv2 is scalable such that it can provide security services for any device, ranging from Personal Digital Assistants (PDAs) to Mainframes, and any operating platform from Windows to UNIX / LINUX. Incorporating the CDSA solution into enterprise environments effectively decouples any single security solution from the infrastructure, and integrates a mechanism (EMM) that allows you to plug and unplug security solutions as required.

CDSA is a security middleware specification and reference implementation that is open source, cross-platform, interoperable, extensible, and freely exportable.

Department of Defense, the Orange book classifications[5] is a set of important guidelines to follow. There are also security related specifications and recommendations from other groups such as BS 7799 / ISO 17799[6], CISSP[7] and Common Criteria[8].

----

[5] The divisions of systems recognized under the trusted computer system evaluation criteria are as follows. Each division represents a major improvement in the overall confidence one can place in the system to protect classified and other sensitive information.

Division (D): Minimal Protection

This division contains only one class. It is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

Division (C): Discretionary Protection

Classes in this division provide for discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate.

Division (B): Mandatory Protection

The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Division (A): Verified Protection

This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development and implementation.

----

[6] **BS 7799 (ISO 17799) - Key Components of the Standard (Extracted from a write up by Biju Mukund, an ISO 17799 / BS 7799 consultant based in India)**

The Standard is divided in two parts:

BS 7799 Part 1 (ISO 17799.2000 Standard) Code of Practice for Information Security Management

BS 7799 Part II Specifies requirements for establishing, implementing and documenting Information Security Management System (ISMS)

The standard has 10 Domains, which address key areas of Information Security Management.

1. **Information Security Policy for the organization.**

   This activity involves a thorough understanding of the organization business goals and its dependence on information security. This entire exercise begins with the creation of an IT Security Policy. This is an extremely important task and should convey total commitment of top management-. The policy cannot be a theoretical exercise. It should reflect the needs of the actual users. It should be implementable, easy to understand and must balance the level of protection with productivity. The policy should cover all the important areas like personnel, physical, procedural and technical.

2. **Creation of information security infrastructure**

A management framework needs to be established to initiate, implement and control information security within the organization. This needs proper procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization.

3. **Asset classification and control**

One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, which is appropriate for copy, store, and transmit or destruction of the information asset.

4. **Personnel Security**

Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training.

Alert and well-trained employees who are aware of what to look for can prevent future security breaches.

5. **Physical and Environmental Security**

Designing a secure physical environment to prevent unauthorized access, damage and interference to business premises and information is usually the beginning point of any security plan. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

6. **Communications and Operations Management**

Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident response procedures.

Network management requires a range of controls to achieve and maintain security in computer networks. This also includes establishing procedures for remote equipment including equipment in user areas. Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks. Special controls may also be required to maintain the availability of the network services.

Exchange of information and software between external organizations should be controlled, and should be compliant with any relevant legislation. There should be proper information and software exchange agreements, the media in transit need to be secure and should not be vulnerable to unauthorized access, misuse or corruption.

Electronic commerce involves electronic data interchange, electronic mail and online transactions across public networks such as Internet. Electronic commerce is vulnerable to a number of network threats that may result in fraudulent activity, contract dispute and disclosure or modification of information. Controls should be applied to protect electronic commerce from such threats.

7. Access control

Access to information and business processes should be controlled on the business and security requirements. This will include defining access control policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication, node authentication, segregation of networks, network connection control, network routing control, operating system access control, user identification and authentication, use of system utilities, application access control, monitoring system access and use and ensuring information security when using mobile computing and tele-working facilities.

8. System development and maintenance

Security should ideally be built at the time of inception of a system. Hence security requirements should be identified and agreed prior to the development of information systems. This begins with security requirements analysis and specification and providing controls at every stage i.e. data input, data processing, data storage and retrieval and data output. It may be necessary to build applications with cryptographic controls. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, protection of cryptographic keys and standards to be used for cryptography.

A strict change control procedure should be in place to facilitate tracking of changes. Any changes to operating system changes, software packages should be strictly controlled. Special precaution must be taken to ensure that no covert channels, back doors or Trojans are left in the application system for later exploitation.

9. Business Continuity Management

A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. This begins by identifying all events that could cause interruptions to business processes and depending on the risk assessment, preparation of a strategy plan. The plan needs to be periodically tested, maintained and re-assessed based on changing circumstances.

10. Compliance

It is essential that strict adherence is observed to the provision of national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and collection of evidence.

Information Technology's use in business has also resulted in enacting of laws that enforce responsibility of compliance. All legal requirements must be complied with to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

BS 7799 (ISO 17799) consists of 127 best security practices (covering 10 Domains which was discussed above) which companies can adopt to build their Security Infrastructure. Even if a company decides not go in for the certification, BS 7799 (ISO 17799) model helps companies maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. Additional benefits of ISMS are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact. Ultimately leads to increased profitability.

[7] CISSP defines the following domains – Access control systems and methodology, Telecommunications, Network & Internet security, Security management practices, Applications and systems development, Cryptography, Security architecture and models, Operations security, Business continuity planning, Law, investigation, ethics and forensics and physical security.

[8] In June 1993, the sponsoring organizations of the existing US, Canadian, and European criteria started the CC Project to align their separate criteria into a single set of IT security criteria. Version 1.0 of the CC was completed in January 1996. Based on a number of trial evaluations and an extensive public review, Version 1.0 was extensively revised and CC Version 2.0 was produced in April of 1998. This became ISO International Standard 15408 in 1999. The CC Project subsequently incorporated the minor changes that had resulted in the ISO process, producing CC version 2.1 in August 1999.

Today the international community has embraced the CC through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of CC evaluations performed by other CCRA members.

The Common Criteria Project is represented on the web at www.CommonCriteriaPortal.org

Common Criteria defines the following two sets of requirements for functional classes and assurance classes.

Common Criteria Functional Classes

Audit, Cryptographic support, Communications, User data protection, Identification and authentication, security management, privacy, protection of security functions, Resource utilization, Access, and Trusted paths and channels.

Common Criteria Assurance Classes

Configuration management, Delivery and operation, Maintenance of assurance, Protection file evaluation, Development, Guidance document, Lifecycle support, Security target evaluation.

Protection Profile (http://niap.nist.gov/pp/index.html)

A Protection Profile (PP) is an implementation-independent specification of information assurance security requirements. Protection profiles are a complete combination of security objectives, security related functional requirements, information assurance requirements, assumptions, and rationale.

The purpose of a PP is to state a security problem rigorously for a given collection of system or products - known as the Target of Evaluation (TOE) - and to specify security requirements to address that problem without dictating how these requirements will be implemented.

Product vendors may respond to the security concerns defined by a PP by producing a Security Target (ST), which is similar to a PP except that it contains implementation-specific information that demonstrate how their product addresses those security concerns.

In accordance with their respective responsibilities under Public Law 100-235 (Computer Security Act of 1987), the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have agreed to cooperate on the development of security requirements for key technology areas necessary for the protection of Federal information systems and networks, including those comprising the critical infrastructure within the United States. NIST and NSA are undertaking this effort:

- To ensure the U.S. Government has a consistent comprehensive set of recommended protection profiles for key technology areas;
- To forge partnerships with public and private sector constituencies to develop and gain consensus on PPs important for critical infrastructure protection; and
- To facilitate national and international convergence of protection profiles in key technology areas.

The following links focus on US Government Protection Profiles and will direct you to either the development process for US Government PPs, Consistency Instruction Manuals for different degrees of robustness, a list of US Government PPs in development, and, finally, a current list of NIAP Validated US Government PPs.

US government's protection profiles (http://niap.nist.gov/cc-scheme/pp/index.html)

Anti-Virus	**Key Recovery**	**PKI/KMI** PP	**Switches and Routers** PP
Biometrics PP PP	**Miscellaneous** PP	**Remote Access** PP	**System Access Control**
Certificate Management PP	**Mobile Code** PP PP	**Secure Messaging** PP	**Tokens** PP
Firewalls PP	**Multiple Domain Solutions** PP	**Security Management**	**Trusted DBS**
Guards PP	**Network Mgmt**	**Sensitive Data Protection**	**VPN** PP
IDS/IPS PP	**Operating System** PP	**Single-Level Web Server** PP	**WLAN** PP
	Peripheral Switch PP	**Smart Cards**	

Notes:
PP= There is a ***Validated U.S. Gov't PP*** available for this technology category of product type. However, it should not be inferred that every product listed within this technology category necessarily meets the PP. You can be redirected to the PP page for the given technology by clicking on the red or black PP icon.

PP= There is a ***draft U.S. Gov't PP*** available for this category of product type. However, it should not be inferred that every product listed within this product type necessarily meets the PP. Draft PPs can be in

SSE-CMM is heavily influenced by the CMMI five layer capability maturity model. OCTAVE is a framework for identifying information security risks. CDSA provides specifications for security middleware.

None of these frameworks consider a holistic view of the vulnerabilities, resulting threats and their combined impact on business, much less attempt to define an index of any kind to represent the state of cyber security health of a business.

This missing link between cyber security risks to their impact on businesses through a maturity model and an index / rating provided us the motivation to pursue the work reported in this document.

The INFOSeMM IT Security Maturity Model framework has been developed with the goal of including all the major factors outlined in the frameworks, specifications and methodologies mentioned above. These well thought out frameworks and methodologies can be applied, either in part or as a whole, in both determining a business' INFOSeMM maturity level and in helping it to progress to a desired level.

various stages of development, i.e., being written or vetted, or in evaluation in a NIAP CCEVS CCTL. You can be redirected to the PP page for the given technology by clicking on the red or black PP icon.

4. The Solution

We examined several frameworks relating to information security and spent several hours of brainstorming and soul searching on what guiding principle should drive our effort. The following risk assessment table appearing in US GAO AI 33[9] document turned out to be the best starting block. US GAO synthesized this table after studying the best practices across industry segments.

Table 1: Risk Assessment Matrix from US Government General Accounting Office

Severity Level	**Probability of Occurrence**				
	Frequent	**Probable**	**Occasional**	**Remote**	**Improbable**
I (high)	A	A	A	B	C
II	A	A	B	B	C
III	A	B	B	C	C
IV (Low)	C	C	D	D	D

Source: US General Accounting Office report GAO / AIMD-00-33 on Risk Assessment Practices

A – Risk 1 (Undesirable and requires **immediate** corrective action)
B – Risk 2 (Undesirable and requires corrective action, but **some management discretion allowed**)
C – Risk 3 (Acceptable with **review by management**)
D – Risk 4 (Acceptable **without review by management**)

We debated and discussed whether the model should capture three, four or five levels of IT security maturity of an organization. However the table in the GAO document helped us settle the debate and it turns out that there was no need for more than four levels.

4.1. The model

We call the four level model INFOSeMM, standing for INFOSYS IT Security Maturity Model. The maturity levels are determined by a business' posture towards reviewing and revising its vulnerabilities along three main dimensions – Infrastructure, Intelligence and Practices. We call these the three pillars of IT security maturity level of any

[9] Information Security Risk Assessment – Practices of leading organizations, GAO/AIMD-00-33, Accounting and Information Management Division, US General Accounting Office.

organization. It is these three pillars that ensure the stability of an organization from an information security perspective.

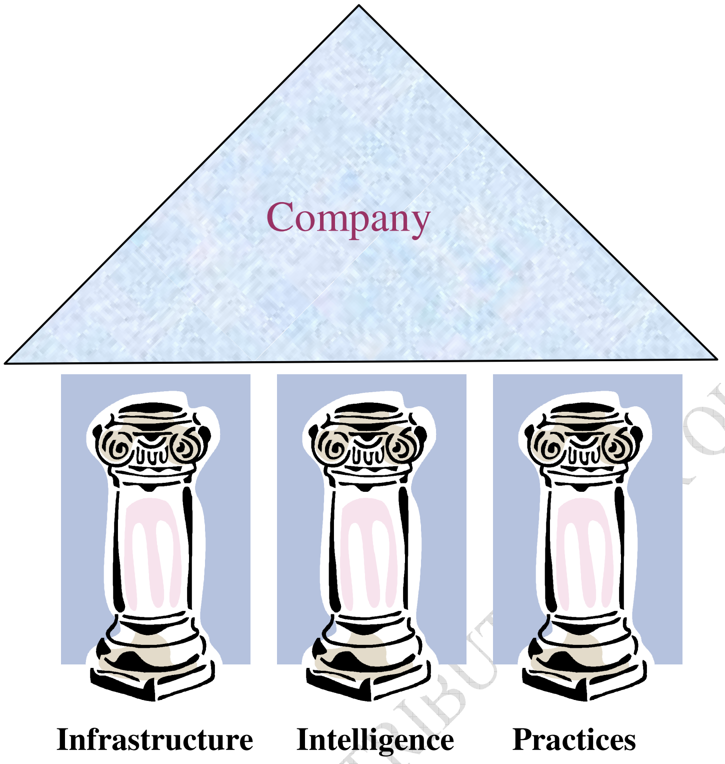

Figure 2: The three information security pillars of a company

Each of the three pillars can in turn be defined in terms of their key components. These definitions are provided below.

a. Infrastructure

We classify the following three under infrastructure vulnerabilities.

- V1 – Network
- V2 – System
- V3 – Environment

Network vulnerabilities will include issues related to firewalls, VPNs, Network forensics, advanced boundary controllers, etc.

System vulnerabilities will include issues related to Operating Systems, Servers, Domains, Security Architecture, etc.

Environment vulnerabilities will include issues related to earthquakes, environmental pollution, terrorism, etc.

b. Intelligence

We classify the following two under Intelligence vulnerabilities.

- V4 – Applications
- V5 – Data

Application vulnerabilities will include issues related to malicious code, application forensics, access control of applications etc.

Data vulnerabilities will include issues related to privacy, confidentiality, unauthorized disclosure, non-delivery or misdelivery of information, etc.

c. Practices

We classify the following three under the Practices vulnerabilities.

- V6 – People
- V7 – Processes
- V8 – Management

People vulnerabilities will include issues such as creating information security awareness amongst employees and others interacting with the company and monitoring the violations and enforcement of the security policies.

Processes will include issues such as creating, maintaining, and retiring information security related policies.

Management will include issues related to risk assessment and mitigation, contingency plans etc.

The following table shows how the different vulnerabilities across the three pillars map into the considerations under different security efforts.

Table 2: Mapping of the eight INFOSeMM vulnerabilities to other frameworks.

IT Security Maturity Level	Testing and Assessment	*Vulnerabilities*							
		Network [V1]	*System [V2]*	*Environment [V3]*	*Application [V4]*	*Data [V5]*	*People [V6]*	*Process [V7]*	*Management [V8]*
Tenets of Security									
Protecting									

Confidentiality						X			
Integrity					X				
Availability			X	X					
Avoiding									
Destruction				X					
Alteration					X	X			
Disruption		X	X	X					
Accountability									X
Non-repudiation			X						
	Test	V1	V2	V3	V4	V5	V6	V7	V8
CISSP Domains									
Access control systems and Methodology			X		X	X			
Telecommunications, Network & Internet Security		X							
Security Management Practices									X
Applications and Systems Development					X				
Cryptography			X						
Security Architecture and Models			X						
Operations Security								X	X
Business Continuity planning				3					
Law, Investigation, Ethics and Forensics								X	X
Physical Security									
	Test	**V1**	**V2**	**V3**	**V4**	**V5**	**V6**	**V7**	**V8**
SSE-CMM									
PA01 Administer Security Controls				X					X
PA02 Assess Impact									
PA03 Assess Security Risk									
PA04 Assess Threat									
PA05 Assess Vulnerability		X	X	X	X	X	X	X	X
PA06 Build Assurance Argument									
PA07 Coordinate Security								X	
PA08 Monitor Security Posture									X?
PA09 Provide Security Input						X?			
PA10 Specify Security Needs									X

PA11 Verify and Validate Security									X
	Test	V1	V2	V3	V4	V5	V6	V7	V8
Common Criteria									
Security Functional Classes (of requirements)									
Audit									4
Cryptographic Support			X						
Communications		X							
User Data Protection						X			
Identification and Authentication								X	
Security Management									X
Privacy						X			
Protection of Security Functions (??)								X	
Resource Utilization									X?
Access (?)			X		X				
Trusted paths / channels		X?							
Security Assurance Classes									
Configuration Management			X						
Delivery and Operation									
Maintenance of Assurance								X	X
Protection profile evaluation (?)								X	X
Development (?)								X	X
Guidance document (?)								X	
Lifecycle support								X	
Security target evaluation (?)								X	
Tests	B1-B4								
Vulnerability assessments	B1-B4	X	X	X	X	X	X	X	X
	Test	V1	V2	V3	V4	V5	V6	V7	V8

4.2. Threats

Vulnerabilities do not lead to risks in isolation. It is the threats in combination with vulnerabilities that lead to business and operational risks. There were initial thoughts on whether the threats ought to influence the maturity index. We finally decided that for the purposes of assessing the IT security maturity it would be most prudent to assume that threats exist at the highest levels. Of course, the extent the threat is real becomes an important consideration when it comes to security related investments.

We discuss the threat – vulnerability relationship later on in this document. At that time we will also discuss the vertical or domain context that needs to be integrated into security planning.

a. Human threats

The following table presents the source, motivation and actions for threats from human beings.

Table 3: Threats from human beings: Source, Motivation and Actions

Source	Motivation	Actions
Hacker, cracker	• Challenge • Ego • Rebellion	• Hacking • Social Engineering • System intrusion, break-ins • Unauthorized system access
Computer Criminal	• Destruction of Information • Illegal information disclosure • Monetary gain • Unauthorized data alteration	• Computer crimes such as cyber-stalking. • Fraud such as replay, impersonation, and interception. • Information bribery • Spoofing • System intrusion
Terrorist	• Blackmail • Destruction • Exploitation • Revenge	• Bomb • Information warfare • DOS, DDOS • System penetration • System tampering
Corporate espionage	• Competitive advantage • Economic advantage	• Access to strategic and competitive proprietary information • Information theft • Intrusion on privacy
Insiders • Poorly trained • Disgruntled • Malicious • Negligent • Dishonest • Terminated	• Curiosity • Ego • Intelligence • Monetary gain • Revenge • Unintentional errors ○ Data entry ○ Programming ○ Unsecured terminals	• Assault on another employee • Blackmail • Browsing unauthorized information • Corrupt / Falsify data • Information theft / bribery • Malicious code • Sale of personal / confidential information • System sabotage

Adapted from: NIST Risk Management Guidelines

b. Threat-Vulnerability relationships

The following table presents some examples of interplay between Vulnerability and Threat.

Table 4: Sample Vulnerability threat relationships

Vulnerability	Threat-source	Threat-action
Employee's system identifiers and privileges are not removed immediately on termination.	Terminated employees who are disgruntled.	• Accessing company proprietary data. • Corrupting company information. • Compromising privacy by accessing data on fellow employees for the purposes of selling or blackmail.
Company firewall allows inbound Telnet and guest ID is enabled on one of the servers.	Unauthorized users including former employees.	Using Telnet to browse using the guest ID.
New security patches are not applied promptly.	Unauthorized users including former employees.	Exploiting known system vulnerabilities to access sensitive information.
Data center uses water sprinklers to suppress fire without providing for suitable cover for hardware and other equipment.	Negligent persons, disgruntled employees or arsonists with no connection to the company.	Hardware ruined when water sprinklers are turned on in the data center.

Adapted from: NIST Risk Management Guidelines

4.3. Domain / Vertical Dependence

The maturity level that an organization should operate in is to a large extent determined by the industry that the company operates in. The following table from Gartner gives the likely hood of a politically motivated attack on critical infrastructure across different industries.

Table 5: Estimates for the likelihood of a politically motivated cyber attack on verticals.

	Comm.	Financial Services	Manufacturing	Utilities	Transport	Government	Other
Very Likely	9.1%	18.8%	23.8%	9.1%	18.2%	37.5%	13.3%
Somewhat likely	40.9%	40.6%	23.8%	36.4%	45.5%	37.5%	40.0%
Total	**50%**	**59.4%**	**47.6%**	**45.5%**	**63.7%**	**75.0%**	**43.3%**

Source: Gartner Research June 2003.

Gartner Research has also carried out analyses on the applications in a vertical that attract attacks. The following table provides one such example for the financial services group.

Table 6: Sample targets for attack in the financial industry

	Cash Flow	Credit	Infrastructure
People	Bank Accounts	Credit cards	Investment Future
Industry	Sales and Receivables	Credit facilities	Infrastructure
Financial markets	Settlements and Transactions	Credit facilities	Depositories and other markets

Source: Gartner research 2003

Hence it is important to customize the maturity level requirements for both a given industry and the applications within that industry.

4.4. Expected benefits from IT Security investments

The basic tenet of security can be classified into protection and avoidance. Protection normally addresses Confidentiality, Integrity and Availability. Avoidance addresses Destruction, Alteration and Disruption. We present the key protection benefits in Table 7, key avoidance benefits in Table 8 and key business benefits in Table 9.

Table 7: Key Benefits from IT security investments for protection purposes

Vulnerabilities secured through IT security investments	Confidentiality	Integrity	Availability
Infrastructure	Protects the network identity thus avoiding incidents such as phishing.	Preserves network and system integrity.	Improves system and network uptime.
Intelligence	Protects privacy and proprietary information.	Preserves data and application integrity.	Improves control of access to applications and data
Practices	Protects process and policy innovations.	Preserves the integrity of policies.	??

Table 8: Key benefits from IT security investments for avoidance purposes

Vulnerabilities secured through IT security investments	Destruction	Alteration	Disruption
Infrastructure	Investment in continuity ensures operations even when destruction is caused by elements of nature or arson.	Investment in Network Address Translation will minimize the hijacking of infrastructure.	Investment in infrastructure redundancy minimizes disruption.
Intelligence	Investment in AAA (Authorization, Access Control and Authentication) and rights management eliminates possible destruction of data and applications.	Investment in AAA (Authorization, Access Control and Authentication) and rights management eliminates possible changes to data and applications.	Investment in hot stand bys ensures 24 x 7 availability of data and applications thus eliminating disruption.
Practices	Investment in Process Management Systems eliminates possible corruption of policies and processes.	Investment in Process Management Systems eliminates possible alteration of policies and processes.	Investment in hot stand bys ensures 24 x 7 availability of policies and processes thus eliminating disruption.

Table 9: Key business benefits from adequate IT security investments.

Vulnerabilities	Impact on Business			
	Business Development	**Regulatory wrath**	**Business Costs**	**Management Time**
Infrastructure	Happy customers become spokespersons for the company.	Compliance with service level requirements saves potential fines and minimizes business disruption.	Service restorations costs are contained.	Management time is freed for strategic decision making.
Intelligence	Customer retention is easier.	Compliance with privacy and confidentiality	Legal costs related to privacy and confidentiality	Management can feel assured that the proprietary and

		requirements saves potential fines and business stoppage.	saved.	personal information is well protected. Results in reduced costs related to potential blackmail.
Practices	New customer acquisition is easier.	Compliance with recommended security policies and standards avoids potential fines and business stoppage.	Contingency plans minimize restoration time. Well thought out policies help reduce insurance premiums.	Accountability processes ensures problems are identified at the earliest and managed well.

4.5. IT Security Maturity Levels

Given that the intent was to ascertain the extent of preparedness of an organization for handling threats from Cyber security attacks, we first needed to find a reasonable representation for the probability of attacks. We were not very comfortable with the GAO's terminology of Frequent, Probable, Occasional, Remote and Improbable. We replaced these with Frequent, Intermittent, Occasional, Rare and Very rare (or negligible). We felt that the revised labeling was less ambiguous than the ones originally used.

We then needed a good system of labeling the responses. Organizations may have been either ignorant of the impact of information security on them or even when they were fully aware may not have the resources to respond. This state will correspond to level 1. Some organizations may have recognized the need to respond to such threats and may have been quite satisfied by committing initial investments. Such organizations are generally classified to be in level 2. Some diligent organizations may have realized the need to address the continuing onslaught of cyber attacks and hence would have instituted regular review and revision of their level of preparedness. These organizations will operate in level 3. Very few organizations might decide to be proactive in their approach to managing such cyber attacks. These organizations will be proactive in anticipating future attacks, drawing up suitable response plans and might even conduct simulated attacks to assess the level of preparedness of their systems and people. These organizations will be operating in level 4 of the Maturity model.

Not all organizations need to operate at level 4. The level at which an organization needs to operate will be largely determined by the industry segment in which it operates. Even where the industry segment requires an organization to operate at the highest level, there may be several applications within an organization which need not operate at the highest levels. For example, if we broadly divide the enterprise applications into internal and external (client and business facing), the internal applications can often operate at a lower maturity level than the external applications.

The four maturity levels for the three pillars are presented in Table 9. The benefits and pains at each of these four maturity levels are presented in Table 10.

Table 10: Maturity levels for the three pillars.

Maturity Level	Infrastructure	Intelligence	Practices	Index range
One: Inactive	Infrastructure (network, system and environment) is not secured.	Intelligence (application and data) is not secured.	Practices (people, process and management) are not secured.	**DDD**
Two: Reactive	Infrastructure is secured in response to incidents.	Intelligence is secured in response to incidents.	Practices are secured in response to incidents.	**cDD, DcD, DDc to CCC**
Three: Streamlined	Infrastructure is secured for known vulnerabilities through regular reviews and resulting revisions. The solutions are streamlined with other two pillars.	Intelligence is secured for known vulnerabilities through regular reviews and resulting revisions. The solutions are streamlined with other two pillars.	Practices are secured for known vulnerabilities through regular reviews and resulting revisions. The solutions are streamlined with other two pillars.	**bCC, CbC, CCb to BBB**
Four: Proactive	Infrastructure is secured for known and anticipated vulnerabilities through regular reviews and resulting revisions.	Intelligence is secured for known and anticipated vulnerabilities through regular reviews and resulting revisions.	Practices are secured for known and anticipated vulnerabilities through regular reviews and resulting revisions.	**aBB, BaB, BBa to AAA**

a. Threat scenarios, likelihoods and impacts

Every business will benefit by using event handling data to model scenarios and prioritize countermeasures. The following table captures the threat scenario, likelihood and impact on systems and business.

Table 11: Threat scenario impacts

Maturity Level	Threat Scenario	Threat Likelihood	Threat Impact on Systems	Threat Impact on Business
One: Inactive	No attention paid to threat scenarios	High to very High	• Significant system disruption • Serious loss of critical proprietary information	• Significant loss of current and future business opportunities • Significant loss of revenues
Two: Reactive	Limited scenario modeling	Medium to high	• Intermittent system disruption • Intermittent loss of proprietary information	• Intermittent loss of current and future business opportunities • Intermittent loss of revenues
Three: Streamlined	Scenario modeling is used to determine priorities of countermeasures	Low to Medium	• Occasional system disruption • Occasional loss of proprietary information	• Occasional loss of current and future business opportunities • Occasional loss of revenues
Four: Proactive	Event handling data is used to revise scenario modeling and prioritization of countermeasures.	Rare to Low	• Rare system disruption • Rare loss of proprietary information	• Rare loss of current and future business opportunities • Rare loss of revenues

b. Business benefits and pains at the four maturity levels.

The benefits and pains that a business will experience while operating at the different levels are listed in the following table.

Table 12: Benefits / pains accruing to a business at different maturity levels

Maturity Level	Benefits	Pains	Concerns
One: Inactive	No benefits.	• Customer morale is very low. High chances of losing existing customers. • New customer acquisitions are extremely difficult. • New product development is severely affected. • Uncontrolled exposure to regulatory fines and hike in insurance premiums. • Unplanned demands on top level management's time. • Significant loss of revenues. • Uncontrolled exposure to blackmail and legal costs arising out of privacy related issues. • Significant reductions in volume of business transactions and revenues.	No company will wish to operate at this level if they can afford to set aside sufficient funds.
Two: Reactive	• Most customers are happy most of the time. • New customer acquisitions are easier. • New product development is mostly unaffected. • Exposure to regulatory fines and hike in insurance	• A few customers are occasionally unhappy. • New customer acquisitions are sometimes difficult. • Occasional problems experienced in new product development. • Partial exposure to hike in insurance premiums. • Possible short term	• The general emphasis is to plug in security holes as and when they are discovered. This approach might be adopted more due to lack of funds for a

	premiums is lowered. • Demand on top management time is significantly reduced. • Loss of revenues is contained. • Exposure to blackmail is contained. • Reduction in the volume of business transactions and revenues contained.	stoppage of business due of lack of total compliance to regulatory requirements. • Demands on mid level management's time. • Moderate reductions in volume of business transactions and revenues	streamlined solution rather than because of lack of appreciation for streamlining. • It might be useful to totally secure individual domains one by one than partially securing all of them.
Three: Streamlined	• Almost all the customers are happy all the time. • New customer acquisition is easy. • Exposure to regulatory fines or hike in insurance premiums is minimal. • Well designed contingency plans significantly reduce the need for management time.	• Minor exposure to blackmail. • Demand on lower level management time. • Minor exposure to legal costs related to privacy issues. • Minor reductions in volume of business transactions and revenues.	• This approach will need more planning and investments. • End to end solutions need to be thought through. • Security solutions should not hamper smooth functioning of businesses.
Four: Proactive	• Existing customers are satisfied and help in the acquisition of new customers. • Exposure to regulatory fines is eliminated. • Insurance premiums can be negotiated down. • Demands on management time	No known pains.	• It is important to understand the ROI on information security investments if a company is in a domain that does not warrant its operations at this level. • All

	eliminated. • Exposure to blackmail and legal costs arising from privacy issues is negligible.		information security solutions should not affect the speed and convenience of usage.

The model is organized into the following components.

I. Firm components
    a. Three pillars.
    b. Four maturity levels.
II. Flexible components
    a. Considerations for determining the maturity level.
    b. Mandatory maturity level for each consideration.
    c. Transition Plans.
    d. Recommended maturity level for an industry vertical.

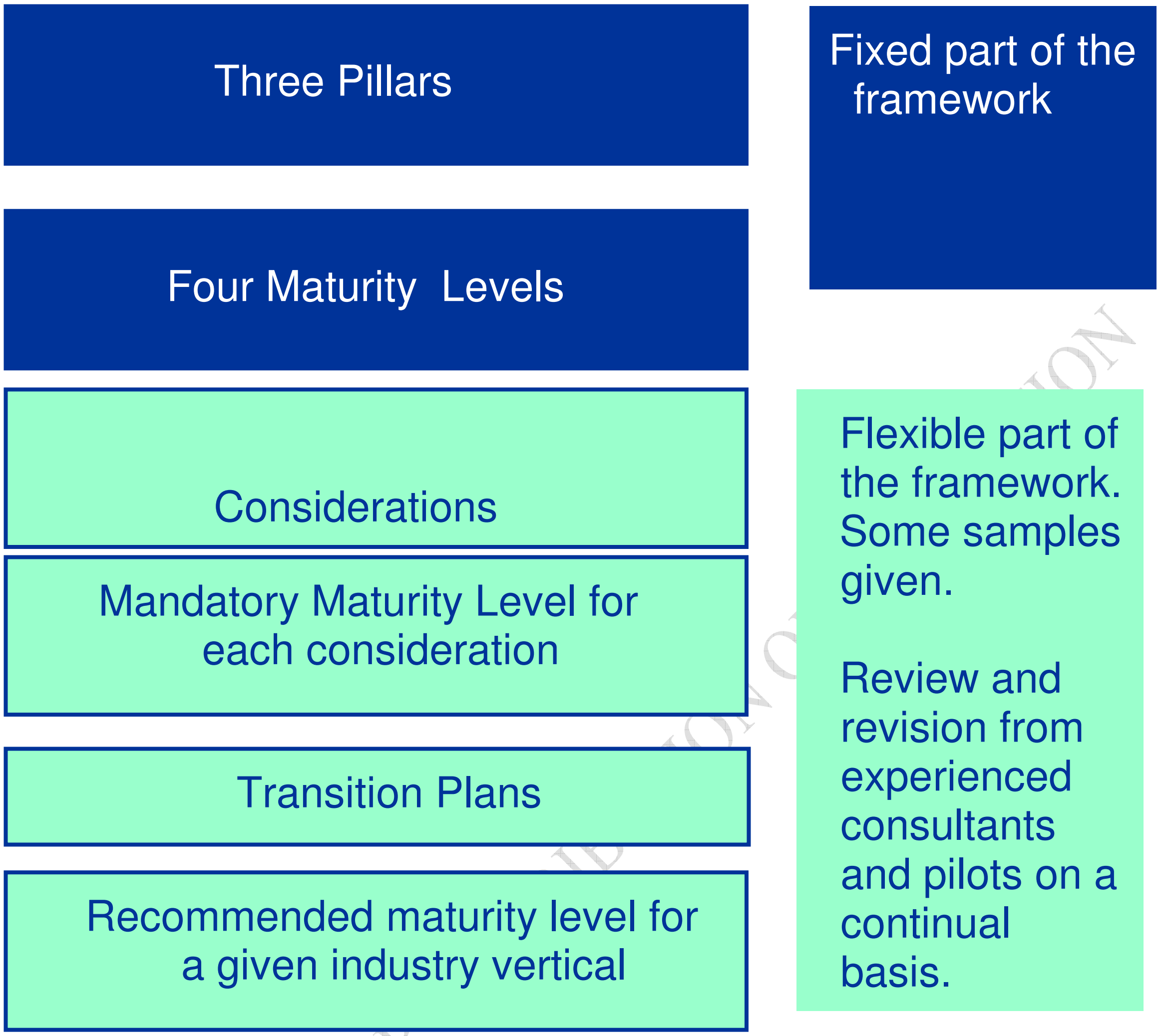
Three Pillars
Four Maturity Levels
Considerations
Mandatory Maturity Level for each consideration
Transition Plans
Recommended maturity level for a given industry vertical
Fixed part of the framework
Flexible part of the framework. Some samples given.
Review and revision from experienced consultants and pilots on a continual basis.

Figure 3: The fixed and variable parts of the INFOSeMM framework.

5. The Transition.

Businesses will first need to assess their current INFOSeMM maturity level. Then they need to decide the maturity level at which they wish to operate[10].

Once the desired maturity level is identified, transition plans to migrate to the desired maturity level need to be drawn up and implemented. Some organizations may prefer to make the transition in small steps in order to optimize the use of their resources. Others might be willing to migrate to the desired level in one step. This is a decision to be made by the executive management team of the organization. Transition plans for the vulnerabilities will include questionnaires that will help assess the current maturity level and the recommended set of actions to be taken to get to the desired maturity level.

a. Maturity Assessment

We have developed a starting set of questionnaires to assess the maturity level of an organization along each of the three pillars. For each pillar, we also provide guidelines for deriving the maturity level.

b. Considerations for the questionnaires

The ideal scenario would be for the set of considerations across all the eight vulnerabilities s be MECE (mutually exclusive and collectively Exhaustive) and that all of them be at the same level of granularity. However, often the nature of considerations for different each of the dimensions will require that some of them be at a different level of granularity than the others. So, this starter set of considerations should be evolved to MECE considerations of near about equivalent granularities.

This is a very tough task, in being able to choose a level of detail, sticking consistently to that level of detail, making sure everything at that level of detail is captured in the questionnaire. The difficulty is compounded by the fact that while there is a vast library of public literature on security, there is no agreed-upon classification, beyond the top level. Also, some of them might cut across more than one dimension. For example, the Management dimension might look at the access control issues and formulate policies which will then be encased in the Practices dimension. Depending upon the type of access control, this consideration will also have to be reflected in either the Application or Data dimension.

Future work might concentrate on a guided descent into the questions, instead of a direct descent. For instance for Network, it would mean, breaking the network into its constituent components.

[10] Infosys consultants should work with their Domain Competency Group to determine the maximum recommended maturity levels for each of the industry verticals. The consultant should also work with the Enterprise Systems group to determine the recommended maturity level for each of the applications in a typical enterprise in each of the verticals.

a. LAN
b. Extranet / VPN
c. Intranet
d. Internet

Then this can perhaps intersect with the maturity level on the following factors:

a. Deployment
b. Deployment & Testing
c. Deployment, Testing and Purchasing / building

One could take the major aspects of user-interaction within each of these stages as the next dimension

a. Identification, Authentication and Authorization
b. Accountability, Non-repudiation
c. Incident handling (Forensics would be discovered if one choose to descend one level lower)

One could develop questions which are points along, one, two or three of the above (dimensions).

A related effort would be to identify the hierarchies under each of the main eight dimensions (Network, Management) such that the sub-dimensions of each of the dimensions at the same level or roughly at the same level of granularity.

Given the short development period and lack of access to the security aware, client facing consultants, we offer the considerations in section 5.1. as an initial starter set. The considerations from which the questionnaires for the eight vulnerabilities across the three pillars need to be maintained by designated security consultants. They need to be reviewed and refined on a regular and proactive basis by designated consultants and disseminated to all other security consultants in the organization to enforce consistency in delivery.

c. Transition Plans

Table 12 presents the set of transition plans that need to be developed in order to migrate any company from the lowest maturity index to the highest maturity index. The transition plans are best developed by the Infosys consultants based on the starter kit of questionnaires used to assess a company's maturity index. Given that the questionnaires are living documents and will be customized for different industries and different client engagements, the transition plans have to be maintained to be in synch with the questionnaires.

d. Ownership

Who owns IT security maturity assessment and transition? Some companies assign the ownership to the IS/ IT groups. Others assign it to a Chief Security Officer. Yet others elevate this to the Chief Risk Officer. The best results have been obtained when the policies are set at the corporate level with inputs from the divisions and the deployment and policy enforcement is made a KPI of all the divisions, business and functional. It is best for each division to report their IT security health during their quarterly reviews on par with their other KPIs such as revenue, profitability, etc. Hence the design and adoption of transition plans should involve the divisions of a company as well.

e. Security and System Development Life Cycle

Security should be considered an integral part of a system development lifecycle. Application development should treat security at a functional level and not at a specific solution / component offering level. For example, an application that treats authentication at a functional level will give itself the flexibility to use solutions as and when they emerge. Those applications that ignore such practices may end up hard coding a specific authentication solution. Such hard coded specific solution based approaches promise to impose significant security related reengineering and maintenance demands on the application.

Table 14. captures the relationship between the Engineering Principles recommended for US Federal Systems Division and the Life Cycle phases. We show how these principles relate to the vulnerabilities (V1 to V8) considered by our maturity model.

Table 13: Transition plans for progressing from one maturity level to the next.

Transitions	Vulnerabilities	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Infrastructure	**Network**	Network vulnerability assessment and transition plan I	Network vulnerability assessment and transition plan II	Network vulnerability assessment and transition plan III
	System	System vulnerability assessment and transition plan I	System vulnerability assessment and transition plan II	System vulnerability assessment and transition plan III
	Environment	Environment vulnerability assessment and transition plan I	Environment vulnerability assessment and transition plan II	Environment vulnerability assessment and transition plan III
Intelligence	**Applications**	Application vulnerability assessment and transition plan I	Application vulnerability assessment and transition plan II	Application vulnerability assessment and transition plan III
	Data	Data vulnerability assessment and transition plan I	Data vulnerability assessment and transition plan II	Data vulnerability assessment and transition plan III
Practices	**People**	People vulnerability assessment and transition plan I	People vulnerability assessment and transition plan II	People vulnerability assessment and transition plan III
	Process	Process vulnerability assessment and transition plan I	Process vulnerability assessment and transition plan II	Process vulnerability assessment and transition plan III
	Management	Management vulnerability assessment and transition plan I	Management vulnerability assessment and transition plan II	Management vulnerability assessment and transition plan III

Table 14: Information Technology Security Engineering principles versus Life-cycle phases (indicates Key to the phase, * optionally used to support the phase)**

Principle (from Federal Systems Guidelines for EP-ITS engineering Principles)	Life-cycle applicability					
	Initiation	Development/ Acquisition	Implementation	Operations/ Maintenance	Disposal	Related Vulnerabilities
1.Establish a sound security policy for design	**	*	*	*	*	**V4**
2. Treat security as an integral part of overall system design.	**	**	**	**	*	**V2**
3. Clearly delineate the physical and logical security boundaries governed by associated security policies		**	*	*		**V7**
4. Reduce risk to an acceptable level	**	**	**	**	**	**V8**
5. Assume that external systems are insecure	**	**	**	**	*	**V1**
6. Identify potential trade-offs between reducing risk and increased costs and decrease in operational effectiveness.	**	**		**		**V8**
7. Implement layered security (Remove any single point of vulnerability)	*	**	*	**	*	**V2**
8. Implement system security measures tailored to meet organizational security goals	*	**	*	**	*	**V8**
9. Strive for simplicity	*	**	*	**		**V7**
10. Design and operate an IT system to limit vulnerability and to be resilient in response.	*	**		**		**V7**
11. Minimize the number of system elements to be trusted.	*	**	*	**		**V7**
12. Implement security through a combination of physical and logical measures.		**	*	*	*	**V8**
13. Provide assurance that the system is, and continues to be, resilient in the face of expected	*	**	*	**	*	**V8**

Principle (from Federal Systems Guidelines for EP-ITS engineering Principles)	Life-cycle applicability					
	Initiation	Development/ Acquisition	Implementation	Operations/ Maintenance	Disposal	Related Vulnerabilities
threats.						
14. Limit or contain vulnerabilities		**	*	*		**V1-V8**
15. Formulate security measures to address multiple overlapping information domains.	*	**	*	*		**V7**
16. Isolate public access systems from mission critical resources.	*	**	*	*		**V2,V1**
17. Use boundary mechanisms to separate computing systems and network infrastructures.		**	*	**		**V2**
18. Where possible base security on open standards for portability and interoperability.	*	**	*			**V7**
19. Use common (layman's) language in developing security requirements.	**	**		**		**V8**
20. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.	*	**	**	*		**V7,V8**
21. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.		**	*	**		**V1,V2**
22. Authenticate users and processes to ensure appropriate access control decisions both within and across domains (and intra, inter and extra nets)	*	*	*	**		**V2,V4**
23. Use unique identities to ensure accountability	*	*	*	**		**V2**
24. Implement least privilege	*	*	*	**		**V7,V2**
25. Do not implement unnecessary security mechanisms	*	**	**	*	*	**V2**
26. Protect information while being processed, in transit and in storage.	*	**	*	**	*	**V1,V4,V5**

Principle (from Federal Systems Guidelines for EP-ITS engineering Principles)	Life-cycle applicability					
	Initiation	Development/ Acquisition	Implementation	Operations/ Maintenance	Disposal	Related Vulnerabilities
27. Strive for operational ease of use	*	**	*	**		**V7**
28. Develop and exercise contingency or disaster recovery procedures To ensure appropriate availability	*	*	*	**		**V3**
29. Consider custom products to achieve adequate security	*	**	*	*		**V2**
30. Ensure proper security in the shut down or disposal of a system		*		*	**	**V7**
31. Protect against all likely classes of “attacks”	*	**	**	*	*	**V7**
32. Identify and prevent common errors and vulnerabilities.		**	**			**V7**
33. Train the developers to write secure software	**	**	*			**V3**

Adapted from: NIST Risk Management Guidelines

5.1. Considerations for developing questionnaires to assess maturity index.

This section presents a starter kit of consideration that can be used for generating the questionnaires to assess the INFOSeMM maturity index of an organization. The questionnaires should identify the gaps between the desired positioning and the current positioning for all the vulnerabilities.

We should emphasize that these considerations are a starter kit. Firstly, they need to be reviewed by consultants for the completeness. We might have included items that the consultants might feel are not very important for certain verticals and we might have omitted some that they would like to introduce for the vertical. Every one of the considerations addressed in the questionnaires should be classified into either mandatory or optional for any level. The level number listed under the column “Maturity Level” indicates the level at which a consideration becomes mandatory. That consideration therefore, by definition, will be optional at the lower levels. These considerations will be used in determining the maturity level of an organization against each of the vulnerabilities. Each of the consideration should be exploded into its components based on the client need.

We use the terms ‘regular or periodic’ and ‘proactive’ when referring to the review and revision of individual features considered through out the different sets of considerations for the questionnaires. The word regular / periodic implies that the reviews and revisions are carried out based on regular time intervals as chosen by an organization. For example, some organizations might choose to review their vulnerabilities every quarter and the others might choose to review semi-annually or even annually. All of these will fall under the category ‘regular’. We use the word ‘proactive’ to indicate that the organizations are committed to review and revise the features as and when needed based on either an alert or an anticipation. Clearly the costs involved in a proactive posture will be more than that involved in a regular posture. This precisely reflects the extent of management commitment to maintain the good IT security health of a company.

When the vulnerabilities are better managed, the business costs of an organization are reduced and the customer and business partner satisfaction levels increased. Satisfied and happy customers and business partners can in turn become the “unpaid” marketing agents for a company’s products and services.

An organization is said to be at a given level of IT security maturity when all the mandatory features at that level are satisfied.

5.1.1. Considerations for generating the questionnaires for assessing the maturity index for the infrastructure pillar.

The infrastructure pillar is made up of three subgroups – Network, System and Environment.

Table 15: Network maturity assessment considerations.

Network maturity related considerations	Level 1	Level 2	Level 3	Level 4	Mandatory maturity level
Intranet[11]	Not secure	Secure	Secure	Secure	2
Internet[12]	Not secure	Not secure	Secure	Secure	3
Extranet[13]	Not secure	Not secure	Not secure	Secure	4
Network disruption	None	Have a passive backup. Cold standby.	Have an active backup. Hot standby.	Proactive disruption planning and management.	As stated
Boundary controllers	None	Basic firewall	Advanced boundary controllers	Adaptive boundary controllers	As stated
Denial of service	None	Denial of service prevention	Denial of service avoidance	Distributed denial of service prevention and avoidance	As stated
Design principles for secure network services and protocols[14]	None	Yes	Reviewed and updated on regular basis	Proactive affordable network security design.	2
Security for collaborative environments	None	For corporate use only	For use within corporate and with customers (CRM apps)	For use within corporate, with customers and business partners	3

[11] Intranet – private enterprise network.

[12] Internet – Global Internet. Enterprise policy can only enforce requirements upon those devices accessing the enterprise network.

[13] Extranet – a protected version of the Enterprise network and is often protected by a Demilitarized Zone (DMZ).

[14] Most enterprise networks are logically separated into the following domain:
User domain – Physical location of the user and the type of network equipment used to access corporate information.
Transport domain – Public and / or part of the enterprise network that is used to connect other domains.
Bastion domain – Webservers, mail gateways, and application gateways.
Data domain – main frames, database servers, and application servers.

Shared services based on Grid computing	None	For corporate use across business functions	For corporate use across business functions and key customers of the client.	For corporate use across business functions key customers, business partners of client.	optional
Deployment, testing and validation of network security tools and mechanisms	Deployed	Deployed. Tested in response to an incident	Deployed. Tested and validated on a regular basis.	Deployed. Proactively tested and validated.	2
Anonymity in networks	None	Static mapping to an IP address	Dynamic IP mapping for fixed durations	Dynamic IP mapping for every transaction	As stated
Accountability in networks	None	Batch audit	Small interval audit	Real time audit	As stated
Network forensics	None	Basic	Advanced	Adaptive (intelligent)	As stated
Method of adoption of new network security technology	None	Ad hoc	Against a defined architecture	Against a seamless extensible architecture	As stated
Streamlining all network security related components	None	Discretionary	Mandatory	Verifiable	3
Business Impact		**Establishes business continuity by managing network and connectivity failures**	**Improves business continuity by minimizing network and connectivity failures**	**Assures business continuity by proactively avoiding network and connectivity failures**	
Mandatory maturity level - Indicates the level from which this consideration becomes mandatory					

Table 16: System maturity assessment considerations.

System maturity related considerations	Level 1	Level 2	Level 3	Level 4	Mandatory maturity level
Operating system	Vanilla	Hardened	Continuous review and update of hardening	Trustworthy authenticated architecture set up	2
Server	Vanilla	Hardened	Continuous review and update of hardening	Trustworthy authenticated architecture set up	2

Middleware	Static	Hardening requirements reviewed on a need basis	Hardening requirements reviewed and revised on a regular basis	Trustworthy authenticated architecture set up	3
IT System	Static	Reviewed on a need basis	Reviewed and revised on a regular basis	Trustworthy authenticated architecture that considers security as integral part of system design	As stated
Security domains	Not addressed	Reviewed on a need basis	Reviewed and revised on a regular basis	Dynamic review and revision	As stated
Securing trust levels	None	Public information secure	Proprietary information secure	Private information secure	As stated
Configuration management	Normal	Reviewed on a need basis	Reviewed and revised on a regular basis	Dynamic review and revision	As stated
Visual rendition of system architecture	None	Basic coarse grain visualization	Fine grain visualization	Demand based dynamically adaptive coarse/fine grain visualization	As stated
Authorization	None	Implemented	Reviewed and revised on a regular basis	Role based and regularly reviewed and revised	2
Access control	None	Fine grained discretionary access control	Mandatory access control	Verified access control	2
Authentication	None	Single factor weak	Two factor strong authentication implemented	Multifactor role based strong authentication implemented	2
End to end encryption	Not verified	Verified at the time of initiation	Regularly reviewed and revised	Verified in real time	3
Installation of latest security patches	Not updated	Updated based on alerts/incidents	Regularly updated	Proactive prioritized updates	2
Backup and recovery	None	Ad hoc batch	Regular and fine grained	Real time fine grained	3
Availability/disruption of systems	No backup provided	Have a passive backup. Cold standby.	Have an active backup. Hot standby.	Proactive disruption planning and management.	As stated
Layered security	Single point of vulnerability exists	Single point of vulnerability minimized	Single point of vulnerability avoided	System updates continue to avoid single point of vulnerability	2

Method of adoption of new systems security technology	None	Ad hoc	Against a defined architecture	Against a seamless extensible architecture	4
Non repudiation	None	Sender verified	Sender and receiver verified	Sender and receiver verification without involvement of trusted third party	As stated
Privacy/Confidentiality	None	Data privacy provided	Data and user privacy provided	User profile protected	As stated
Streamlining all system security related components	None	Discretionary	Mandatory	Verifiable	3
Business Impact		**Establishes business continuity by managing consequences due to system disruption or damage and loss of proprietary information**	**Improves business continuity by minimizing system disruption and damage and loss of proprietary information**	**Assures business continuity by proactively avoiding consequences due to system disruption and damage and loss of proprietary information**	
Mandatory maturity level **-** Indicates the level from which this activity becomes mandatory					

Table 17: Environment maturity assessment considerations.

Environment maturity related considerations	Level 1	Level 2	Level 3	Level 4	Mandatory maturity level
Disaster management plan	None	Implemented	Implemented and regularly reviewed and revised	Implemented and proactively reviewed and revised	2
Provision for resumption of lost service	None	Cold site implemented	Cold and hot site implemented	Cold and hot site proactively reviewed and revised	A stated
Duplicated critical systems and applications	None	Implemented	Implemented and regularly reviewed and revised	Implemented and proactively reviewed and revised in real-time	2
Communications lines	Single	Duplicate paths established	Multiple paths established	Multiple paths established and proactively reviewed and revised	As stated
Storage and backup of critical data	Onsite only	Offsite storage implemented sporadic backups	Backup at offsite on a regular basis	Backup at Offsite on a real-time basis	As stated

Rotate backup media	Not done	Done on monthly basis	Done on a weekly basis	Done on a daily basis	2
Test the disaster management plan	Not done	Implemented	Implemented and regularly reviewed and revised	Implemented and proactively reviewed and revised	As stated
Recovery of data and services	One day	Few hours	Few minutes to an hour	Instantaneous	2
Monitoring potential disasters	Ad hoc	Weekly	Daily	Hourly	2
Streamlining all environmental components that affect information security	Not implemented	Discretionary	Mandatory	Verifiable	3
Business Impact		**Establishes business continuity by managing consequences due to potential environmental disaster.**	**Improves business continuity by minimizing consequences due to potential environmental disaster.**	**Assures business continuity by proactively avoiding consequences due to potential environmental disaster.**	
Mandatory maturity level - Indicates the level from which this consideration becomes mandatory					

5.1.2. Considerations for generating the questionnaires for assessing the maturity index for the intelligence pillar.

The Intelligence pillar is made up two subgroups – Applications and Data.

Table 18: Considerations for Application maturity assessment.

Application maturity related considerations	Level 1	Level 2	Level 3	Level 4	Mandatory maturity level
Security Wrappers for legacy applications	None	some legacy applications provided with security wrappers	All legacy applications with regular review and revision of definition of legacy	All legacy applications with proactive review and revision of definition of legacy	3
Malicious Code Detection	Not implemented	Implemented	Implemented with regular review and revision	Implemented real time with proactive review and revision	2
End to end information flow certification	Not implemented	Discretionary	Implemented with regular review and revision	Verified real time with proactive review and revision	3
Application audit for information security compliance and integrity	Not implemented	Discretionary	Implemented with regular review and revision	Verified with proactive review and revision	3
Application forensics	Not implemented	Implemented	Implemented with regular review and revision	Verified real time with proactive review and revision	2
Revision control of sensitive applications	Not implemented	Implemented	Implemented with regular review and revision	Verified with proactive review and revision	2
Information security and Application Development Methodology	As an afterthought	Integrated into SDLC (ISIDLC - Information security integrated SDLC)	ISIDLC regularly reviewed and revised to maintain compatibility with new IT security solutions	ISIDLC proactively reviewed and revised to maintain compatibility with new IT security solutions	2

Access control of applications	Not implemented	Implemented	Implemented with regular review and revision	Verified with proactive review and revision	2
Application availability	Single point of failure	Have a passive backup. Cold standby.	Have an active backup. Hot standby.	Proactive disruption planning and management.	As stated
Sensitivity level of the applications	No application sensitivity tables created and maintained	Some application sensitivity tables created.	Application sensitivity tables created and maintained with regular review and revision	Application sensitivity tables created and maintained with proactive review and revision	3
Path between application and information storage	Unsecured	Partially secured	Path security regularly reviewed and revised	Path security proactively reviewed and revised	3
Streamlining all application security related components	Nor implemented	Discretionary	Mandatory	Verifiable	3
Business Impact		**Establishes business retention and growth through application availability and protection against malicious code**	**Improves business retention and growth through streamlined application availability and protection against malicious code**	**Assures business retention and growth through proactive management of application availability and protection against malicious code**	
***Mandatory maturity level* - Indicates the level from which this consideration becomes mandatory**					

Table 19: Considerations for data maturity assessment.

Data maturity related considerations	Level 1	Level 2	Level 3	Level 4	Mandatory maturity level
Separation of users and data	not considered	mandatory	mandatory	verifiable	2
Labeling of major data structures	not considered	discretionary	mandatory	verifiable	3
Integrity of labels for the data structures	not considered	discretionary	discretionary	verifiable	4
Sensitivity analyses of the data (protection -critical Vs. Non protection -critical)	not considered	mandatory	mandatory	verifiable	2

data integrity	not considered	mandatory	mandatory	verifiable	2
Rights management	not considered	mandatory	mandatory	verifiable	2
Fine grain access control of data	not considered	discretionary	mandatory	verifiable	3
User access of data	direct	mediated with mandatory access control	mediated with mandatory access control	mediated with verifiable access control	As stated
data audit	not considered	mandatory	mandatory	verifiable	2
mechanisms to prevent unauthorized disclosure of data	not considered	discretionary	mandatory	verifiable	3
Mechanisms to prevent non-delivery of data	not considered	discretionary	mandatory	verifiable	3
Mechanisms to prevent mis-delivery of data	not considered	discretionary	mandatory	verifiable	3
Mechanisms for preventing the inadvertent destruction of data	not considered	mandatory	mandatory	verifiable	2
Mechanisms for preventing the inadvertent modification of data	not considered	mandatory	mandatory	verifiable	2
Data encryption for storage	not considered	mandatory	mandatory	verifiable	2
Data encryption for communication	not considered	mandatory	mandatory	verifiable	2
Application independent data flow	not considered	discretionary	mandatory	verifiable	3
Streamlining all data security related components	not considered	discretionary	mandatory	verifiable	3
Business Impact		**Ensures business growth by managing the potential loss of critical proprietary information**	**Improves business growth by minimizing the loss of critical and other proprietary information**	**Assures business growth by avoiding the loss of critical proprietary and private information**	
***discretionary (level 2*)** **-** divisions are aware of the needs and are given the discretion to adopt and implement the feature; review and revision is discretionary					
discretionary (level 3) **-** divisions are aware of the needs and are given the discretion to adopt and implement the feature; regular review and revision is mandatory					
mandatory **(*level 2)*** **-** all divisions are aware of the needs and are required to adopt and implement the feature; regular review and revision is discretionary					

mandatory (level 3) - all divisions are aware of the needs and are required to adopt and implement the feature; regular review and revision is mandatory
Verifiable - all divisions are aware of the needs and are required to adopt and implement the feature and are also required to provide verifiable evidence that the implementation and efficacy; proactive review and revision is mandatory
Mandatory maturity level - Indicates the level from which this consideration becomes mandatory

5.1.3. Considerations for generating the questionnaires for assessing the maturity index for the Practices pillar.

The practices pillar consists of three subgroups – People, Processes and Management.

Table 20: Considerations for people maturity assessment

People Maturity related considerations	Level 1	Level 2	Level 3	Level 4	Mandatory maturity level
Information security awareness	not implemented	mandatory implementation	mandatory implementation	verifiable implementation	2
Security training requirements	not implemented	mandatory implementation	mandatory implementation	verifiable implementation	2
Training targets	not identified	mandatory implementation	mandatory implementation	verifiable implementation	2
Training compliance	not implemented	discretionary implementation	mandatory implementation	verifiable implementation	3
User accountability for login procedures	not implemented	discretionary implementation	mandatory implementation	verifiable implementation	3
User accountability for virus updates	not implemented	discretionary implementation	mandatory implementation	verifiable implementation	3
User accountability for timely upgrades and other patches	not implemented	discretionary implementation	mandatory implementation	verifiable implementation	3
Briefing of information security policy updates	not implemented	mandatory implementation	mandatory implementation	verifiable implementation	2
Incidence response training	not implemented	mandatory implementation	mandatory implementation	verifiable implementation	2
Consequences of security policy violations	not implemented	mandatory implementation	mandatory implementation	verifiable implementation	2
Security policy violation enforcements	not implemented	discretionary implementation	mandatory implementation	verifiable implementation	3
User acknowledgement of security policy requirements	not implemented	discretionary implementation	mandatory implementation	verifiable implementation	3
Streamlining all user related IT security components	not implemented	discretionary implementation	mandatory implementation	verifiable implementation	3

Business Impact		**Manages business losses due to willful or inadvertent security violations at all touch points.**	**Minimizes business losses due to willful or inadvertent security violations at all touch points.**	**Assures avoidance of business losses due to willful or inadvertent security violations at all touch points.**	
discretionary implementation - managers have the discretion to decide which employees are covered; review and revision is also discretionary					
mandatory implementation (level 2) - all employees must covered; regular review and revision is discretionary					
mandatory implementation (level 3) - all employees must covered; regular review and revision is mandatory					
verifiable implementation - implies random tests to verify the training etc.; proactive review and revision is mandatory					
Mandatory maturity level **-** Indicates the level from which this consideration becomes mandatory					

Table 21: Considerations for process maturity assessment.

Process maturity related considerations	Level 1	Level 2	Level 3	Level 4	Mandatory maturity level
Process for generating the taxonomies of security domains	not implemented	mandatory	mandatory	verifiable	2
Process for building resilient systems	not implemented	discretionary	mandatory	verifiable	3
Process for real-time detection of attacks and interdiction	not implemented	discretionary	mandatory	verifiable	3
Process for determining most likely attacks	not implemented	discretionary	mandatory	verifiable	3
Process for determining countermeasures	not implemented	discretionary	mandatory	verifiable	3
Process for threat scenario simulation and forecasting	not implemented	discretionary	discretionary	verifiable	4
Process for threat prioritization	not implemented	discretionary	mandatory	verifiable	3
Process for adversary classification and mitigation	not implemented	discretionary	discretionary	verifiable	4

strategy					
Processes for risk identification and mitigation	not implemented	mandatory	mandatory	verifiable	2
Policies for information security management	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for distributing defense point	not implemented	mandatory	mandatory	verifiable	2
Regulatory policies and processes	not implemented	mandatory	mandatory	verifiable	2
Advisory policies and processes	not implemented	discretionary	mandatory	verifiable	3
Informative policies and processes	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for authentication services	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for installation of latest security patches	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for virus protection software	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for software hardening	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for hardware hardening	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for server segmentation	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for latest upgrades and service packs	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for entitlement services	not implemented	mandatory	mandatory	verifiable	2

Policies and processes for verification services	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for Privacy services	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for back up	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for recovery	not implemented	mandatory	mandatory	verifiable	2
policies and processes for incident response	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for checking compliances	not implemented	discretionary	mandatory	verifiable	3
Policies and processes for disaster management	not implemented	discretionary	mandatory	verifiable	3
Policies and processes for non repudiation	not implemented	discretionary	mandatory	verifiable	3
Policies and processes for aligning physical and cyber securities	not implemented	discretionary	mandatory	verifiable	3
Policies and processes for monitoring and adoption of emerging information security related standards, frameworks and methodologies	not implemented	discretionary	mandatory	verifiable	3
Policies and processes for enforcement	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for monitoring vulnerabilities	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for risk management	not implemented	mandatory	mandatory	verifiable	2

Policies and processes for security coordination	not implemented	discretionary	mandatory	verifiable	3
Policies and processes for protecting security functions	not implemented	discretionary	mandatory	verifiable	3
Policies and processes for configuration management	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for operational risk management	not implemented	discretionary	mandatory	verifiable	3
Policies and processes for maintenance of assurance	not implemented	discretionary	mandatory	verifiable	4
Policies and processes for protection profile evaluation	not implemented	mandatory	mandatory	verifiable	2
Policies and processes for security target evaluation	not implemented	discretionary	mandatory	verifiable	2
Policies and processes for ownership of all security related policies and processes	not implemented	discretionary - corporate level	mandatory - corporate level	verifiable - corporate level	2
Streamlining IT security related policies and processes	Not implemented	discretionary	mandatory	verifiable	3
Business Impact		**Establishes management of business continuity and growth problems by defining appropriate processes and policies.**	**Minimizes business continuity and growth related problems by constant review and revision of security processes and policies.**	**Avoids business continuity and growth related problems by proactive review and revision of security processes and policies.**	

discretionary (level 2) - divisions are aware of the needs but are given the discretion to adopt and implement policies and processes; review and revision is discretionary

discretionary (level 3) - divisions are aware of the needs but are given the discretion to adopt and implement policies and processes; regular review and revision is mandatory

mandatory (level 2) - all divisions are aware of the needs and are required to adopt and implement the policies and processes; regular review and revision is discretionary

mandatory (level 3) - all divisions are aware of the needs and are required to adopt and implement the policies and processes; regular review and revision is mandatory

Verifiable - all divisions are aware of the needs and are required to adopt and implement the policies and processes and are also required to provide verifiable evidence that the implementation and efficacy; proactive review and revision is mandatory

Mandatory maturity level **-** Indicates the level from which this consideration becomes mandatory

Table 21: Considerations for assessment of Management maturity.

Management maturity related considerations	Level 1	Level 2	Level 3	Level 4	Mandatory maturity level
Division level accountability	not managed	discretionary management	mandatory management	verifiable management	3
Risk assumption	not managed	mandatory management	mandatory management	verifiable management	2
Risk avoidance	not managed	discretionary management	mandatory management	verifiable management	3
Risk limitation	not managed	mandatory management	mandatory management	verifiable management	2
Risk planning	not managed	mandatory management	mandatory management	verifiable management	2
Risk research	not managed	discretionary management	discretionary management	mandatory, verifiable management	4
Risk transference	not managed	mandatory management	mandatory management	verifiable management	2
Preventive management security controls	not managed	discretionary management	mandatory management	verifiable management	3
Detection management security controls	not managed	mandatory management	mandatory management	verifiable management	2
Recovery management security controls	not managed	mandatory management	mandatory management	verifiable management	2
Security categorization	not managed	mandatory management	mandatory management	verifiable management	2
Security functional requirements	not managed	mandatory management	mandatory management	verifiable management	2
Security assurance requirements	not managed	mandatory management	mandatory management	verifiable management	2

Security requirements assessment and planning		mandatory management	mandatory management	verifiable management	2
Security certification	not managed	discretionary management	mandatory management	verifiable management	3
Security accreditation	not managed	discretionary management	mandatory management	verifiable management	3
Disposal	not managed	discretionary management	mandatory management	verifiable management	3
Disaster management planning	not managed	discretionary management	mandatory management	verifiable management	3
Assured outsourcing	not managed	discretionary management	discretionary management	verifiable management	4
Risk reward analyses	not managed	discretionary management	discretionary management	verifiable management	4
Streamlining all security related management	not managed	Discretionary management	Mandatory management	Verifiable management	3
Business Impact		**Establishes a framework for managing security related business risks**	**Minimizes security related business risks by constantly reviewing and revising the framework**	**Avoids security related business risks by proactively reviewing and revising the framework.**	
Discretionary management (level 2) - Scope, review and revision is at the discretion of the divisional level managements					
Discretionary management (level 3) - Scope is at the discretion of the divisional level managements, regular review and revision is mandatory					
Mandatory management (level 2) - Scope is predefined, review and revision is discretionary					
Mandatory management (level 3) - Scope is predefined, regular review and revision is mandatory					
Verifiable management - Scope is predefined and proactive verifiable review and revisions					
***Mandatory maturity level* -** Indicates the level from which this consideration becomes mandatory					

5.1.4. Methodology for deriving INFOSeMM maturity ratings.

Let us recall how we derived maturity rating / index for each of the three pillars.

Deriving a maturity rating for infrastructure.

Network and systems have to be streamlined and hence will together form the minimum block for the infrastructure pillar. Hence, the rating at levels 2, 3, and 4 will not be bumped up if only one of these two is satisfied. Environmental disruptions can have an effect on the other two components and hence needs to be handled separately.

If the level 2 requirements are satisfied for Network and Systems, then the rating for the infrastructure pillar is a 'c'. If the level 2 requirements are satisfied for all the subgroups then the rating for the infrastructure pillar is a 'C'.

If the level 3 requirements are satisfied for Network and Systems, then the rating for the infrastructure pillar is a 'b'. If the level 3 requirements are satisfied for all the subgroups then the rating for the infrastructure pillar is a 'B'.

If the level 4 requirements are satisfied for Network and Systems, then the rating for the infrastructure pillar is an 'a'. If the level 4 requirements are satisfied for all the subgroups then the rating for the infrastructure pillar is an 'A'.

Deriving a maturity rating for intelligence pillar.

Intelligence pillar is made up of Applications and data. Both need to be secured. However, there is really no preferred order of securing them. We bump up the rating into a small case rating at the next level if only one of them is satisfied.

If the level 2 requirements are satisfied for Applications or Data, then the rating for the intelligence pillar is a 'c'. If the level 2 requirements are satisfied for both the subgroups then the rating for the intelligence pillar is a 'C'.

If the level 3 requirements are satisfied for Applications or Data, then the rating for the intelligence pillar is a 'b'. If the level 3 requirements are satisfied for both the subgroups then the rating for the intelligence pillar is a 'B'.

If the level 4 requirements are satisfied for Network and Systems, then the rating for the intelligence pillar is an 'a'. If the level 4 requirements are satisfied for both the subgroups then the rating for the intelligence pillar is an 'A'.

Deriving a maturity rating for Practices.

Processes subgroup is the most important of the three. There is no means of ensuring security if the processes are not implemented even if the other two subgroups are implemented. Hence the ratings do not change if the Processes subgroup is not satisfied. When the processes subgroup alone is satisfied we bump up the rating to a small case letter at the next level. Once the processes subgroup is satisfied, the other two (people and management) need to be satisfied in order for the rating to be changed to an upper case letter. Some people might prefer that not just processes but that combined with management should form the minimum block. This has to be examined before adoption.

If the level 2 requirements are satisfied for Processes subgroup alone, then the rating for the practices pillar is a 'c'. If the level 2 requirements are satisfied for all the subgroups then the rating for the practices pillar is a 'C'.

If the level 3 requirements are satisfied for Processes subgroup alone, then the rating for the practices pillar is a 'b'. If the level 3 requirements are satisfied for all the subgroups then the rating for the practices pillar is a 'B'.

If the level 4 requirements are satisfied for Processes subgroup alone, then the rating for the practices pillar is an 'a'. If the level 4 requirements are satisfied for all the subgroups then the rating for the practices pillar is an 'A'.

Minimum and Maximum Maturity ratings at different levels.

Level 1

The only maturity rating at Level 1 is DDD.

Level 2

The minimum maturity rating in this level will be cDD or DcD or DDc and the maximum maturity rating is CCC.

Level 3

The minimum maturity rating in this level will be bCC or CbC or CCb and the maximum maturity rating is BBB.

Level 4

The minimum maturity rating in this level will be aBB or BaB or BBa and the maximum maturity rating is AAA.

5.2. Transition plans.

Transition plans help migrate a company from the current maturity level to the desired maturity level[15]. This migration might happen through a few intermediate steps or through a single giant step. The migration strategy will be influenced by the type of organization and their priorities. Also companies might choose to selectively migrate to higher levels for some of the considerations.

Inactive to Reactive transitions (also called transition plan I)

This is where Infosys might have the greatest consulting and follow on IT services business potential. Migrating from the inactive to reactive levels will require "filling the security gaps". The consulting assignments will involve asking the right questions to determine the maturity level along each of the three pillars. A starter set of questions have been presented under the "Consideration for questionnaires" section. A consultant needs to customize the questions to match the industry and the client. The consultant will use eight customized questionnaires to identify the gaps in each of the eight vulnerabilities V1 to V8.

As is evident from this list, the study will encompass all the eight vulnerabilities. Proposed solutions might be ad-hoc and piece meal to satisfy the budgetary constraints or the commitment levels of the organization.

Reactive to Streamlined transitions (also called transition plan II)

This transition consists of two subsets. First subset will consist of those considerations are being addressed for the first time. The second subset will consist of those considerations addressed in the earlier transition and will require periodic review and revision. Periodic review and revision should be conducted at regular intervals. Each consideration might require a different period of regularity. For example, some of the considerations might be revisited every year; where as those considered more important might be reviewed every six months or even every quarter. The client facing consultants will have to decide on the appropriate intervals based on the industry domain the client belongs to and customer's sensitivity to the review and revision intervals.

In this transition, the consultant should also study the interdependencies of the different vulnerabilities and whether they have been streamlined so that the one upstream that is the weakest link does not compromise the goodness created by the well secured link downstream. Also, the streamlining effort should ensure that there is a well matched information flow without any jams created in intermediate points – Jams due to security breaches or simply the performance characteristics of the different devices in the chain.

Streamlined to Proactive transitions (also called transition plan III)

[15] These transition plans are derived from and are dependent on the considerations in sections 5.1.1.1 through 5.1.3.3. Any changes in those considerations will alter the transition plans accordingly.

This transition also consists of two subsets. First subset will consist of those considerations are being addressed for the first time. The second subset will consist of those considerations addressed in the earlier transitions and will require key alert based review and revision. Key alert based review and revision will not wait for the next review and revision period. The management of the company has to define and agree the set of key alert events for each of the considerations. When a key alert event happens, it should trigger a review and revision. The client facing consultants will have to advise the type of events that should be classified as key alerts. These will be influenced by the industry domain that the company operates in and the level of a company's commitment to security. A highly proactive company in an incident sensitive industry domain will normally choose to include a large number of events in its key alert set.

5.2.1. Network Transition Plans.

Network transition has three plans – inactive to reactive, reactive to streamlined and streamlined to proactive. The considerations listed are a starter set. They need to be validated by security consultants with their own past experience and future client engagements.

5.2.1.1. Inactive Level to Reactive Level.

This transition addressed topics related to securing a company's internal network.

	Table 22: Areas of focus for Network Transition Plan I
1	Intranet.
2	Network disruption – passive back up.
3	Basic boundary controllers.
4	Denial of service – prevention.
5	Design principles for secure network services and protocols.
6	Shared services based on Grid computing – across enterprise divisions.
7	Deployment, testing and validation of network security tools and mechanisms
8	Anonymity in networks –static mapping.
9	Accountability in networks – batch audit
10	Basic network forensics
11	Ad Hoc method of adoption of new network security technology

5.2.1.2. Reactive Level to Streamlined Level.

This transition introduces topics such as a company's external network addressing its customers.

	Table 23: Areas of focus for Network Transition Plan II
1	Internet.
2	Network disruption.
3	Advanced boundary controllers.
4	Denial of service – avoidance.
5	Periodic review of design principles for secure network services and protocols.
6	Security for collaborative environments for enterprise divisions and key customers.
7	Shared services based on Grid computing for enterprise and its key customers.
8	Periodic review and revisions of deployment, testing and validation of network security tools and mechanisms
9	Anonymity in networks – dynamic IP mapping during on selected bases.
10	Accountability in networks – Short interval audit.
11	Advanced network forensics
12	Method of adoption of new network security technology
13	Streamlining all network security related components

5.2.1.3. Streamlined to Proactive Level.

This transition introduces topics such as securing a company's external network for business partners.

	Table 24: Areas of focus for Network Transition Plan III
1	Extranet.
2	Network disruption – proactive, key alert based review and revision.
3	Adaptive boundary controllers
4	Denial of service – Distributed attack management.
5	Design principles for secure network services and protocols – affordable network designs.
6	Security for collaborative environments - corporate, customer and business partner.
7	Shared services based on Grid computing – divisions, customers and business partners.
8	Proactive testing and validation of deployment, testing and validation of network security tools and mechanisms based on key alerts.
9	Anonymity in networks – Dynamic IP mapping for every transaction.
10	Accountability in networks – Real time audit.
11	Network forensics – Adaptive.
12	Method of adoption of new network security technology – Seamless extensible architecture.
13	Streamlining all network security related components – key alert based review and revision for verifiability.

5.2.2. System Transition Plans.

System transition has three plans – inactive to reactive, reactive to streamlined and streamlined to proactive. The considerations listed are a starter set. They need to be validated by security consultants with their own past experience and future client engagements.

5.2.2.1. Inactive to Reactive Level.

This transition addresses a minimum set of areas needed to secure systems.

	Table 25: Areas of focus for system transition plan I
1	Operating system
2	Server
3	IT System security - reviewed on a need basis
4	Security domains – reviewed on a need basis
5	Securing trust levels – Public information
6	Configuration management – reviewed on a need basis
7	Visual rendition of system architecture – coarse grain
8	Identity Management
9	Authorization
10	Access control – Fine grained discretionary
11	Authentication – weak, single factor
12	Installation of latest security patches – incident based
13	Availability/disruption of systems – Cold standby
14	Layered security – Minimize single point of vulnerability
15	Non repudiation – Sender verified
16	Privacy/Confidentiality – data confidentiality

5.2.2.2. Reactive to Streamlined Level.

This transition introduces areas such as proprietary information and fine grained visualization of information security architectures.

	Table 26: Areas of focus for system transition plan II
1	Operating system – periodic review
2	Server – periodic review
3	Middleware – hardening
4	IT System security – periodic review and revision
5	Security domains – periodic review and revision
6	Securing trust levels – proprietary information
7	Configuration management – periodic review and revision
8	Visual rendition of system architecture – fine grain
9	Identity Management
10	Authorization – periodic review and revision

11	Access control
12	Authentication – strong authentication (two factor)
13	End to end encryption – periodic review and revision
14	Installation of latest security patches – periodic review and revision
15	Backup and recovery – fine grained
16	Availability/disruption of systems – active back up
17	Layered security – single point of vulnerability avoided
18	Non repudiation – Sender and receiver verified
19	Privacy/Confidentiality – data confidentiality and user privacy
20	Streamlining all system security related components

5.2.2.3. Streamlined to Proactive Level.

This transition introduces areas such as seamless extensible architectures and securing private information.

	Table 27: Areas of focus for system transition plan III
1	Operating system – key alert based review and revision for verifiability
2	Server – key alert based review and revision for verifiability
3	Middleware – key alert based review and revision for verifiability
4	IT System security – trustworthy architecture
5	Security domains – key alert based review
6	Securing trust levels – private information
7	Configuration management – key alert based review and revision for verifiability
8	Visual rendition of system architecture – dynamically adaptable hybrid
9	Identity Management
10	Authorization – Role based
11	Access control – key alert based review and revision for verifiability
12	Authentication – adaptive authentication including multi factor solutions
13	End to end encryption – verifiable in real time
14	Installation of latest security patches – key alert based review and revision for verifiability
15	Backup and recovery – real time, fine grained
16	Availability/disruption of systems – proactive disruption management planning.
17	Layered security – single point of vulnerability sensitive updates
18	Method of adoption of new systems security technologies – seamless extensible architecture
19	Non repudiation – Sender and receiver verified without a the need of a trusted third party
20	Privacy/Confidentiality – data confidentiality, user privacy, user profile protection.
21	Streamlining all system security related components – key alert based review and revision for verifiability.

5.2.3. Environment Transition Plans.

Environment transition has three plans – inactive to reactive, reactive to streamlined and streamlined to proactive. The considerations listed are a starter set. They need to be validated by security consultants with their own past experience and future client engagements.

5.2.3.1. Inactive to Reactive Level.

This transition addresses the minimum set of issues related to environment.

	Table 28: Areas of focus for environment Transition Plan I
1	Disaster management plan
2	Provision for resumption of lost service – cold stand by
3	Duplicated critical systems and applications
4	Communications lines – duplicate paths established
5	Storage and backup of critical data – sporadic
6	Rotate backup media – monthly cycle
7	Test the disaster management plan
8	Recovery of data and services – within few hours
9	Monitoring potential disasters – weekly

5.2.3.2. Reactive to Streamlined Level.

This transition addresses robust back up for business continuity.

	Table 29: Areas of focus for environment Transition Plan II
1	Disaster management plan – periodic review and revision
2	Provision for resumption of lost service – Hot and Cold standbys
3	Duplicated critical systems and applications – periodic review and revision
4	Communications lines - multiple paths established
5	Storage and backup of critical data – at regular intervals
6	Rotate backup media – weekly
7	Test the disaster management plan – periodic review and revision
8	Recovery of data and services – few minutes to less than an hour
9	Monitoring potential disasters - daily
10	Streamlining all security components affected by environmental factors

5.2.3.3. Streamlined to Proactive Level.

This transition focuses mainly on proactive business continuity planning related topics.

	Table 30: Areas of focus for environment Transition Plan III
1	Disaster management plan – key alert based review and revision for verifiability
2	Provision for resumption of lost service – key alert based review and revision for verifiability
3	Duplicated critical systems and applications – proactive and real time where required

4	Communications lines – optimized multiple paths
5	Storage and backup of critical data – in real time
6	Rotate backup media – daily
7	Test the disaster management plan – key alert based review and revision for verifiability
8	Recovery of data and services – instantaneous
9	Monitoring potential disasters – hourly or less
10	Streamlining all security components affected by environmental factors – key alert based review and revision for verifiability.

5.2.4. Applications Transitions Plans.

Application transition has three plans – inactive to reactive, reactive to streamlined and streamlined to proactive. The considerations listed are a starter set. They need to be validated by security consultants with their own past experience and future client engagements.

5.2.4.1. Inactive to Reactive Level.

This transition addresses minimum set of application security related topics.

	Table 31: Areas of focus for Application Transition Plan I
1	Security Wrappers for legacy applications - selected
2	Malicious Code Detection
3	Application forensics
4	Revision control of sensitive applications
5	Information security and Application Development Methodology - Integrated
6	Access control of applications
7	Application availability – cold standby

5.2.4.2. Reactive to Streamlined Level.

This transition introduces areas such as end to end information certification, application sensitivity and audit.

	Table 32: Areas of focus for Application Transition Plan II
1	Security Wrappers for all legacy applications
2	Malicious Code Detection – periodic review and revision
3	End to end information flow certification – periodic review and revision
4	Application audit for information security compliance and integrity – periodic review and revision
5	Application forensics – periodic review and revision
6	Revision control of sensitive applications – periodic review and revision
7	Information security and Application Development Methodology - periodic review and revision
8	Access control of applications – periodic review and revision
9	Application availability - active standby
10	Sensitivity level of the applications – periodic review and revision
11	Secure path between application and information storage – periodic review and revision
12	Streamlining all application security related components

5.2.4.3. Streamlined to Proactive Level.

This transition focuses mainly on key alert based review and revision for all the areas introduced earlier.

	Table 32: Areas of focus for Application Transition Plan III
1	Security Wrappers for legacy applications – current applications designed legacy proof
2	Malicious Code Detection – key alert based review and revision for verifiability.
3	End to end information flow certification – key alert based review and revision for verifiability
4	Application audit for information security compliance and integrity – key alert based review and revision for verifiability
5	Application forensics – key alert based review and revision for verifiability.
6	Revision control of sensitive applications – key alert based review and revision for verifiability
7	Information security and Application Development Methodology – key alert based review and revision for verifiability.
8	Access control of applications – key alert based review and revision for verifiability.
9	Application availability – key alert based review and revision for verifiability.
10	Sensitivity level of the applications – key alert based review and revision for verifiability.
11	Secure path between applications and information storage – key alert based review and revision for verifiability.
12	Streamlining all application security related components – key alert based review and revision for verifiability.

5.2.5. Data Transitions Plans

Data transition has three plans – inactive to reactive, reactive to streamlined and streamlined to proactive. The considerations listed are a starter set. They need to be validated by security consultants with their own past experience and future client engagements.

5.2.5.1. Inactive to Reactive Level.

This transition addresses a minimum set of data security related topics.

	Table 33: Areas of focus for data transition plan I
1	Separation of users and data
2	Sensitivity analyses of the data (protection -critical Vs. Non protection - critical)
3	data integrity
4	Rights management
5	User access of data
6	Data audit
7	Mechanisms for preventing the inadvertent destruction of data
8	Mechanisms for preventing the inadvertent modification of data
9	Data encryption for storage
10	Data encryption for communication

5.2.5.2. Reactive to Streamlined Level.

This transition introduces issues related to data delivery and advanced data protection.

	Table 34: Areas of focus for data transition plan II
1	Separation of users and data – periodic review and revision
2	Labeling of major data structures – periodic review and revision
3	Sensitivity analyses of the data – periodic review and revision
4	data integrity – periodic review and revision
5	Rights management – periodic review and revision
6	Fine grain access control of data – periodic review and revision
7	User access of data – periodic review and revision
8	Data audit – periodic review and revision
9	Mechanisms to prevent unauthorized disclosure of data – periodic review and revision
10	Mechanisms to prevent non-delivery of data – periodic review and revision
11	Mechanisms to prevent mis-delivery of data – periodic review and revision
12	Mechanisms for preventing the inadvertent destruction of data – periodic review and revision
13	Mechanisms for preventing the inadvertent modification of data – periodic review and revision
14	Data encryption for storage – periodic review and revision
15	Data encryption for communication – periodic review and revision
16	Application independent data flow – periodic review and revision
17	Streamlining all data security related components

5.2.5.3. Streamlined to Proactive Level.

This transition focuses on the integrity of the labels for key data structures and the key alert based review and revision of all areas introduced earlier.

	Table 35: Areas of focus for data transition plan III
1	Separation of users and data – key alert based review and revision for verifiability
2	Labeling of major data structures - key alert based review and revision for verifiability
3	Integrity of labels for the data structures - key alert based review and revision for verifiability
4	Sensitivity analyses of the data - key alert based review and revision for verification
5	data integrity - key alert based review and revision for verifiability
6	Rights management - key alert based review and revision for verifiability
7	Fine grain access control of data - key alert based review and revision for verifiability
8	User access of data - key alert based review and revision for verifiability
9	data audit - key alert based review and revision for verifiability
10	mechanisms to prevent unauthorized disclosure of data - key alert based review and revision for verifiability
11	Mechanisms to prevent non-delivery of data - key alert based review and revision for verifiability
12	Mechanisms to prevent mis-delivery of data - key alert based review and revision for verifiability
13	Mechanisms for preventing the inadvertent destruction of data - key alert based review and revision for verifiability
14	Mechanisms for preventing the inadvertent modification of data - key alert based review and revision for verifiability
15	Data encryption for storage - key alert based review and revision for verifiability
16	Data encryption for communication - key alert based review and revision for verifiability
17	Application independent data flow - key alert based review and revision for verifiability
18	Streamlining all data security related components – key alert based review and revision for verifiability.

5.2.6. People Transition Plans

People transition has three plans – inactive to reactive, reactive to streamlined and streamlined to proactive. The considerations listed are a starter set. They need to be validated by security consultants with their own past experience and future client engagements.

5.2.6.1. Inactive to Reactive Level.

This transition introduces areas such as basic employee training including consequences of security policy violations.

	Table 36: Areas of focus for people transition plan I
1	Information security awareness
2	Security training requirements
3	Training targets
4	Briefing of information security policy updates
5	Incidence response training
6	Consequences of security policy violations

5.2.6.2. Reactive to Streamlined Level.

This transition introduces user accountability related topics.

	Table 37: Areas of focus for people transition plan II
1	Information security awareness - periodic review and revision
2	Security training requirements - periodic review and revision
3	Training targets - periodic review and revision
4	Training compliance - periodic review and revision
5	User accountability for login procedures - periodic review and revision
6	User accountability for virus updates - periodic review and revision
7	User accountability for timely upgrades and other patches - periodic review and revision
8	Briefing of information security policy updates - periodic review and revision
9	Incidence response training - periodic review and revision
10	Consequences of security policy violations - periodic review and revision
11	Security policy violation enforcements - periodic review and revision
12	User acknowledgement of security policy requirements - periodic review and revision
13	Streamlining all people related components for information security

5.2.6.3. Streamlined to Proactive Level.

This transition focuses entirely on key alert based review and revision of all the areas introduced earlier.

	Table 38: Areas of focus for people transition plan
1	Information security awareness - key alert based review and revision for verifiability
2	Security training requirements - key alert based review and revision for verifiability
3	Training targets - key alert based review and revision for verifiability
4	Training compliance - key alert based review and revision for verifiability
5	User accountability for login procedures - key alert based review and revision for verifiability
6	User accountability for virus updates - key alert based review and revision for verifiability
7	User accountability for timely upgrades and other patches - key alert based review and revision for verifiability
8	Briefing of information security policy updates - key alert based review and revision for verifiability
9	Incidence response training - key alert based review and revision for verifiability
10	Consequences of security policy violations - key alert based review and revision for verifiability
11	Security policy violation enforcements - key alert based review and revision for verifiability
12	User acknowledgement of security policy requirements - key alert based review and revision for verifiability
13	Streamlining all people related components for information security – key alert based review and revision for verifiability.

5.2.7. Processes Transition Plans

Process transition has three plans – inactive to reactive, reactive to streamlined and streamlined to proactive. The considerations listed are a starter set. They need to be validated by security consultants with their own past experience and future client engagements.

5.2.7.1. Inactive to Reactive Level.

This transition processes and policies for the most basic information security management.

	Table 39: Areas of focus for Processes transition plan I
1	Process for generating the taxonomies of security domains
2	Processes for risk identification and mitigation
3	Policies for information security management
4	Policies and processes for distributing defense point
5	Regulatory policies and processes
6	Informative policies and processes
7	Policies and processes for authentication services
8	Policies and processes for installation of latest security patches
9	Policies and processes for virus protection software
10	Policies and processes for software hardening
11	Policies and processes for hardware hardening
12	Policies and processes for server segmentation
13	Policies and processes for latest upgrades and service packs
14	Policies and processes for entitlement services
15	Policies and processes for verification services
16	Policies and processes for Privacy services
17	Policies and processes for back up
18	Policies and processes for recovery
19	policies and processes for incident response
20	Policies and processes for enforcement
21	Policies and processes for monitoring vulnerabilities
22	Policies and processes for risk management
23	Policies and processes for configuration management
24	Policies and processes for protection profile evaluation
25	Policies and processes for security target evaluation
26	Policies and processes for ownership of all security related policies and processes

5.2.7.2. Reactive to Streamlined Level.

This transition introduces new topics such as policies and processes for attack detection and countermeasures, regulatory compliance, disaster management, and aligning physical and cyber security solutions.

	Table 40: Areas of focus for Processes transition plan II
1	Process for generating the taxonomies of security domains - periodic review and revision
2	Process for building resilient systems
3	Process for real-time detection of attacks and interdiction
4	Process for determining most likely attacks
5	Process for determining countermeasures
6	Process for threat prioritization
7	Processes for risk identification and mitigation - periodic review and revision
8	Policies for information security management - periodic review and revision
9	Policies and processes for distributing defense point - periodic review and revision
10	Regulatory policies and processes - periodic review and revision
11	Advisory policies and processes
12	Informative policies and processes - periodic review and revision
13	Policies and processes for authentication services - periodic review and revision
14	Policies and processes for installation of latest security patches - periodic review and revision
15	Policies and processes for virus protection software - periodic review and revision
16	Policies and processes for software hardening - periodic review and revision
17	Policies and processes for hardware hardening - periodic review and revision
18	Policies and processes for server segmentation - periodic review and revision
19	Policies and processes for latest upgrades and service packs - periodic review and revision
20	Policies and processes for entitlement services - periodic review and revision
21	Policies and processes for verification services - periodic review and revision
22	Policies and processes for Privacy services - periodic review and revision
23	Policies and processes for back up - periodic review and revision
24	Policies and processes for recovery - periodic review and revision
25	policies and processes for incident response - periodic review and revision
26	Policies and processes for checking compliances
27	Policies and processes for disaster management
28	Policies and processes for non repudiation
29	Policies and processes for aligning physical and cyber security solutions
30	Policies and processes for monitoring and adoption of emerging information security related standards, frameworks and methodologies
31	Policies and processes for enforcement - periodic review and revision
32	Policies and processes for monitoring vulnerabilities - periodic review and revision
33	Policies and processes for risk management - periodic review and revision
34	Policies and processes for security coordination
35	Policies and processes for protecting security functions
36	Policies and processes for configuration management - periodic review and revision
37	Policies and processes for operational risk management
38	Policies and processes for protection profile evaluation - periodic review and revision
39	Policies and processes for security target evaluation - periodic review and revision.
40	Policies and processes for ownership of all security related policies and processes - periodic review and revision.
41	Streamlining all policies and processes related to information security.

5.2.7.3. Streamlined to Proactive Level.

This transition introduces processes for threat simulation and forecasting and adversary classification with the necessary mitigation strategies.

	Table 41: Areas of focus for Processes transition plan III
1	Process for generating the taxonomies of security domains - key alert based review and revision for verifiability
2	Process for building resilient systems - key alert based review and revision for verifiability
3	Process for real-time detection of attacks and interdiction - key alert based review and revision for verifiability
4	Process for determining most likely attacks - key alert based review and revision for verifiability
5	Process for determining countermeasures - key alert based review and revision for verifiability
6	Process for threat scenario simulation and forecasting - key alert based review and revision for verifiability
7	Process for threat prioritization - key alert based review and revision for verifiability
8	Process for adversary classification and mitigation strategy - key alert based review and revision for verifiability
9	Processes for risk identification and mitigation - key alert based review and revision for verifiability
10	Policies for information security management - key alert based review and revision for verifiability
11	Policies and processes for distributing defense point - key alert based review and revision for verifiability
12	Regulatory policies and processes - key alert based review and revision for verifiability
13	Advisory policies and processes - key alert based review and revision for verifiability
14	Informative policies and processes - key alert based review and revision for verifiability
15	Policies and processes for authentication services - key alert based review and revision for verifiability
16	Policies and processes for installation of latest security patches - key alert based review and revision for verifiability
17	Policies and processes for virus protection software - key alert based review and revision for verifiability
18	Policies and processes for software hardening - key alert based review and revision for verifiability
19	Policies and processes for hardware hardening - key alert based review and revision for verifiability
20	Policies and processes for server segmentation - key alert based review and revision for verifiability
21	Policies and processes for latest upgrades and service packs - key alert based review and revision for verifiability
22	Policies and processes for entitlement services - key alert based review and revision for verifiability
23	Policies and processes for verification services - key alert based review and revision for verifiability
24	Policies and processes for Privacy services - key alert based review and revision for verifiability
25	Policies and processes for back up - key alert based review and revision for verifiability
26	Policies and processes for recovery - key alert based review and revision for verifiability
27	Policies and processes for incident response - key alert based review and revision for verifiability
28	Policies and processes for checking compliances - key alert based review and revision for verifiability

29	Policies and processes for disaster management - key alert based review and revision for verifiability
30	Policies and processes for non repudiation - key alert based review and revision for verifiability
31	Policies and processes for aligning physical and cyber security solutions - key alert based review and revision for verifiability
32	Policies and processes for monitoring and adoption of emerging information security related standards, frameworks and methodologies - key alert based review and revision for verifiability
33	Policies and processes for enforcement - key alert based review and revision for verifiability
34	Policies and processes for monitoring vulnerabilities - key alert based review and revision for verifiability
35	Policies and processes for risk management - key alert based review and revision for verifiability
36	Policies and processes for security coordination - key alert based review and revision for verifiability
37	Policies and processes for protecting security functions - key alert based review and revision for verifiability
38	Policies and processes for configuration management - key alert based review and revision for verifiability
39	Policies and processes for operational risk management - key alert based review and revision for verifiability
40	Policies and processes for maintenance of assurance - key alert based review and revision for verifiability
41	Policies and processes for protection profile evaluation - key alert based review and revision for verifiability
42	Policies and processes for security target evaluation - key alert based review and revision for verifiability
43	Policies and processes for ownership of all security related policies and processes - key alert based review and revision for verifiability
44	Streamlining all policies and processes related to information security – key alert based review and revision for verifiability.

5.2.8. Management Transition Plans

Management transition has three plans – inactive to reactive, reactive to streamlined and streamlined to proactive. The considerations listed are a starter set. They need to be validated by security consultants with their own past experience and future client engagements.

5.2.8.1. Inactive to Reactive Level

This transition mainly addresses basic risk management and security requirements.

	Table 42: Areas of focus for Management transition plan I
1	Risk assumption
2	Risk limitation
3	Risk planning
4	Risk transference
5	Detection management security controls
6	Recovery management security controls
7	Security categorization
8	Security functional requirements
9	Security assurance requirements
10	Security requirements assessment and planning

5.2.8.2. Reactive to Streamlined Level

This transition introduces new areas such as risk avoidance, preventive management of security controls, disposal management and disaster management planning.

	Table 43: Areas of focus for Management transition plan II
1	Division level accountability
2	Risk assumption- periodic review and revision
3	Risk avoidance
4	Risk limitation - periodic review and revision
5	Risk planning - periodic review and revision
6	Risk transference - periodic review and revision
7	Preventive management security controls
8	Detection management security controls - periodic review and revision
9	Recovery management security controls - periodic review and revision
10	Security categorization - periodic review and revision
11	Security functional requirements - periodic review and revision
12	Security assurance requirements - periodic review and revision
13	Security requirements assessment and planning - periodic review and revision
14	Security certification
15	Security accreditation
16	Disposal
17	Disaster management planning
18	Streamlining all security management related components.

5.2.8.3. Streamlined to Proactive Level

This transition introduces new areas such as risk research, risk reward analyses and assured outsourcing.

	Table 44: Areas of focus for Management transition plan III
1	Division level accountability - key alert based review and revision for verifiability
2	Risk assumption - key alert based review and revision for verifiability
3	Risk avoidance - key alert based review and revision for verifiability
4	Risk limitation - key alert based review and revision for verifiability
5	Risk planning - key alert based review and revision for verifiability
6	Risk research - key alert based review and revision for verifiability
7	Risk transference - key alert based review and revision for verifiability
8	Preventive management security controls - key alert based review and revision for verifiability
9	Detection management security controls - key alert based review and revision for verifiability
10	Recovery management security controls - key alert based review and revision for verifiability
11	Security categorization - key alert based review and revision for verifiability
12	Security functional requirements - key alert based review and revision for verifiability
13	Security assurance requirements - key alert based review and revision for verifiability
14	Security requirements assessment and planning - key alert based review and revision for verifiability
15	Security certification - key alert based review and revision for verifiability
16	Security accreditation - key alert based review and revision for verifiability
17	Disposal - key alert based review and revision for verifiability
18	Disaster management planning - key alert based review and revision for verifiability
19	Assured outsourcing - key alert based review and revision for verifiability
20	Risk reward analyses - key alert based review and revision for verifiability
21	Streamlining all security management related components – key alert based review and revision for verifiability.

6. Business opportunities for Infosys

Infosys can generate both consulting and IT services business opportunities using the framework presented in this report. Some examples of business opportunities[16] are presented in tables 14.1 through 14.8.

Table 45: Business opportunities for Infosys in the network maturity domain.

Nature of Business opportunity	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Consulting	• Security assessment, benchmarking and recommendations for migration. • Design principles for secure network services and protocols. • Assessment for the need of secure Grid computing for shared services. • Information security audit requirements. • Ad-hoc methods for adoption of new security technologies.	• Security assessment benchmarking and recommendations for migration. • Review of design principles for secure network services and protocols. • Study on secure collaborative platform development. • Review deployment, testing and validation of network tools and mechanisms.	• Security assessment benchmarking and recommendations for migration. • Cost-benefit analysis of proactive disruption planning and management. • Affordable network security design. • Recommendations for real-time audit (for selected industries)
IT services	Design, Development and Deployment of: • Secure Intranet. • Boundary controller. • Passive standby. • Basic denial of service solutions. • Secure shared services on Grid computing platforms for enterprise use. • Network anonymity solutions.	Design, Development and Deployment of: • Secure Internet implementation. • Hot standby. • Advanced boundary controllers. • Secure collaborative environments. • Denial of service avoidance. • Secure Grid based	Design, Development and Deployment of: • Secure extranet implementation. • Adaptive boundary controllers. • Distributed denial of service (multi-point attack) prevention and avoidance. • Secure collaboration

[16] These business opportunities are derived from and are dependent on the considerations listed in sections 5.1.1.1 through 5.1.3.3. Any changes in those considerations will accordingly alter the list of business opportunities.

	- Network tools and mechanisms. - Basic network forensics.	shared services for business partners. - Revised and streamlined deployment, testing and validation of network security tools and mechanisms. - Advanced network forensics	environment for extranets. - Real-time fine-grained network anonymity. solutions. - Real-time fine-grained audit. - Adaptive network forensics.

Table 46: Business opportunities for Infosys in the system maturity domain.

Nature of Business opportunity	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Consulting	- Security assessment, benchmarking and recommendations for migration. - Incidence based review of IT system security. - Incidence based review of configuration management. - AAA (Authentication, Authorization and Access control including identity management) - Patch management. - Plans for back up and recovery. - Study to minimize single point of vulnerability. - Study requirements for data privacy.	- Security assessment, benchmarking and recommendations for migration. - Periodic review of IT system security. - Periodic review of configuration management. - Periodic review of AAA. - Review of end to end encryption. - Periodic review of patch management. - Plans for fine grained back up and recovery. - Study to avoid single point of vulnerability. - Study requirements for client privacy. - Study to streamline all system security related topics.	- Security assessment, benchmarking and recommendations for migration. - Advanced review of Trustworthy[17] IT systems. - Key alert based review of configuration management. - Key alert based review of AAA. - Prioritization oriented patch management. - Prioritization based real time fine grained back up and recovery. - Study to maintain the prevention of single point of vulnerability. - Study of a seamless and extensible system architecture for the adoption of new security technologies.

			- Study requirements for client profile privacy.
IT services	Design, Development and Deployment of: - Hardened OS. - Hardened servers. - Security domains. - Systems for securing public information. - Simple AAA. - Coarse grain visualization of security architecture (including a dashboard including INFOSeMM rating). - Business continuity solutions for intranet. based applications. - Non-repudiation of sender.	Design, Development and Deployment of: - Hardened middleware. - Fine grain visualization of security architecture. - Two factor based strong AAA. - End to end work and information flow platforms - Business continuity solutions for intranet and internet based applications. - Non-repudiation of sender and receiver using a trusted third party. - Streamlined implementation of system security. Review and revise: - Security domains at regular intervals.	Design, Development and Deployment of: - Seamless, extensible security middleware. - Adaptive (fine grain for regions of interest and coarse grain for others) visualization of security architecture. - Multi factor based stronger AAA. - Verifiable end to end work and information flow platforms. - Business continuity plans for internet, intranet and extranet based applications. - Seamless architecture for the adoption of new security technologies. - Non-repudiation of sender and receiver without the need for a trusted third party. Review and revise: - Security domains in response to key alerts.

Table 47: Business opportunities for Infosys in the environment maturity domain.

Nature of Business opportunity	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Consulting	- Security assessment, benchmarking and recommendations	- Security assessment, benchmarking and recommendations for	- Security assessment, benchmarking and recommendations for

	for migration. - Natural disasters management plan.	migration. - Periodic review of natural disaster management plan. - Study to streamline the different environment related components that impact IT security.	migration. - Exceptional review of natural disaster management plan based on key alerts.
IT services	Design, Development and Deployment of: - Natural disaster management system (including monitoring). - Storage, back up and restoration systems for critical applications and data. - Disaster management simulation and testing system.	Periodic review and revision of - Natural disaster management system at regular intervals. - Storage, back up and restoration systems for critical applications and data. - Disaster simulation and testing system. - Streamlined environment management system for IT security.	Key alert based review and revision of - Natural disaster management systems. - Storage, back up and restoration systems for critical applications and data. - Disaster simulation and testing system.

Table 48: Business opportunities for Infosys in the application maturity domain.

Nature of Business opportunity	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Consulting	- Security assessment, benchmarking and recommendations for migration. - Addressing security requirements of legacy applications on a need basis. - Study of malicious code detection methods. - Study of application	- Security assessment, benchmarking and recommendations for migration. - Study of the security requirements of all legacy applications - End to end information flow security certification. - Application audit for information security	- Security assessment, benchmarking and recommendations for migration. - Application development methodology that separates the application from the security technology as a preemptive approach to preventing future

	forensics requirements. • Study of revision and access control of sensitive applications. • Study and adopt an Information Security integrated System Development Life Cycle (ISISDLC). • Study to implement application availability. • Vertical / domain dependent application sensitivity. • Methods to secure the path between application and storage.	compliance and integrity. • Study for streamlining all application security related components. Periodic review and revision of: • Study of malicious code detection methods. • Application forensics requirements. • Revision and access control of sensitive applications. • ISISDLC. • Application availability. • Vertical / domain dependent application sensitivity. • Methods to secure the path between application and storage.	legacy issues for current applications. Key alert based review and revision of: • Study of malicious code detection methods. • End to end information flow security certification. • Application audit for information security compliance and integrity. • Application forensics requirements. • Revision and access control of sensitive applications. • ISISDLC. • Application availability. • Vertical / domain dependent application sensitivity. • Methods to secure the path between application and storage.
IT services	Design, Development and Deployment of: • Security wrappers for selected legacy applications. • Malicious code detection solutions. • Applications forensics. • Revision and access control of sensitive applications. • Systems for application availability.	Design, Development and Deployment of: • Security wrappers for all legacy applications. Periodic review and revision of: • Malicious code detection solutions. • Application forensics. • Revision and access control of sensitive applications. • Systems for application	Design, Development and Deployment of: • Key alert based review and revision of: • Malicious code detection solutions. • Application forensics. • Revision and access control of sensitive applications. • Systems for applications availability. • Solution for securing

	• Solution for securing the path between application and data.	availability. • Solution for securing the path between applications and data. • Streamlined application security management.	the path between applications and data.

Table 49: Business opportunities for Infosys in the data maturity domain.

Nature of Business opportunity	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Consulting	• Security assessment, benchmarking and recommendations for migration. • Study to optimize the separation of data and users (Orange book C1). • Study identifying protection critical and non-protection critical data. • Study on data integrity. • Study on data protection.	• Security assessment, benchmarking and recommendations for migration. • Study on sensitivity labeling of major data structures (Orange book B). • Study on data delivery. • Study on application independent data flow. • Study for streamlining all components related to data security. Periodic review and revision of: • Separation of data and users.	• Security assessment, benchmarking and recommendations for migration. • Study of integrity of sensitivity labeling (Orange book B). Study on verifiability of: • Data analyses and labeling. • Data integrity. • Data delivery. • Data protection. • Separation of data from users and applications.
IT services	Design, Development and Deployment of: • Separation of data and users (Orange Book C1). • Tools for sensitivity analyses of data. • Systems to protect data integrity including prevention of inadvertent destruction or	Design, Development and Deployment of: • Sensitivity labeling of major data structures. • Data domains based on protection critical and non-protection critical divisions. • Robust data delivery systems that prevent non-delivery, mis-delivery and	Design, Development and Deployment of: • Systems for integrity preservation of data sensitivity labeling. • Fine grain verifiable access control of data. Verification systems for: • Sensitivity labeling of major data structures. • Rights management.

	alteration of data. • Data encryption for storage and communications. • Data audit systems. • Rights management of data. • Discretionary mediated access control of data.	unauthorized disclosure of data. • Fine grain mandatory mediated access control of data. • Application independent information flow. • Streamlined data security management system. Periodic review and revision of: • Separation of data and users. • Data audit systems. • Data encryption systems. • Systems for preserving data integrity.	• Data delivery. • Data protection. • Data integrity. • Separation of data, users and applications. • Data audit.

Table 50: Business opportunities for Infosys in the people maturity domain.

Nature of Business opportunity	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Consulting	• Security assessment, benchmarking and recommendations for migration. • Information security awareness training requirements and training targets. • Information security policy and violation consequences.	• Security assessment, benchmarking and recommendations for migration. • Information security awareness training requirements and targets compliance testing. • User accountability for login procedures, timely installation of security upgrades and patches. • User acknowledgement of security policy requirements and enforcement of	• Security assessment, benchmarking and recommendations for migration. • Study for the verifiability of: • Information security awareness training requirements, training targets and their compliance. • User accountability for login procedures, timely installation of security upgrades and patches. • Use acknowledgement of

		violations. - Study to streamline all security components related to people. Periodic review and revision of: - Information security awareness training requirements and training targets. - User accountability for login procedures, timely installation of security upgrades and patches.	security policy requirements and enforcements of violations.
IT services	Design, Development and Deployment of: - Information security awareness training.	Design, Development and Deployment of: - Systems to capture and analyze user accountability for login procedures, timely installation of security upgrades and patches. - Streamlined people security management system. Periodic review and revision of: - Information security awareness training.	Design, Development and Deployment of: - Systems for verification of information security awareness training, policy briefing, user acknowledgement, and user accountability.

Table 51: Business opportunities for Infosys in the practices maturity domain.

Nature of Business opportunity	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Consulting	- Security assessment, benchmarking and recommendations for migration. - Taxonomy of security domains. - Policies and processes for	- Security assessment, benchmarking and recommendations for migration. - Building resilient systems - Threat scenario simulation, most	- Security assessment, benchmarking and recommendations for migration. - Threat forecasting. Verification studies of: - Taxonomy of security

	information security management including people training, adoption of regulatory inputs, identity management, entitlement services, verification services, privacy services, installation of security updates and patches, software/ hardware hardening and server segmentation, configuration management, backup, recovery and restoration, vulnerability monitoring, protection profile evaluation, security target evaluation, and incidence response. • Policies and processes for risk identification and management, and violation enforcement. • Policies and processes for identifying owners for all the information security related policies and processes.	likely attack forecasting, adversary classification, planning countermeasures, real time attack detection, and response prioritization. • Policies and processes for prioritized countermeasures, information security compliance, disaster and business continuity management, non-repudiation, adoption of emerging solutions and standards, aligning physical and information security solutions, security coordination, advisory policies, protecting security functions and operational risk management. • Study to streamline all IT security related policies. Periodic review and revision of: • Policies and processes for information security management including people training, adoption of regulatory inputs, identity management, entitlement services, verification services, privacy services, installation of	domains. • Real time attack detection and response prioritization. • Policies and processes for information security management including people training, adoption of regulatory inputs, identity management, entitlement services, verification services, privacy services, installation of security updates and patches, software/ hardware hardening and server segmentation, configuration management, backup, recovery and restoration, vulnerability monitoring, protection profile evaluation, security target evaluation, and incidence. • Policies and processes for prioritized countermeasures, information security compliance, disaster and business continuity management, non-repudiation, adoption of emerging solutions and standards, aligning physical and information security

		security updates and patches, software/ hardware hardening and server segmentation, configuration management, backup, recovery and restoration, vulnerability monitoring, protection profile evaluation, security target evaluation, and incidence.	solutions, security coordination, advisory policies, protecting security functions and operational risk management. • Resilient systems • Threat scenario simulation, most likely attack forecasting, adversary classification, planning countermeasures, real time attack detection, and response prioritization. •
IT services	Design, Development and Deployment of: • Security domains. • Processes for information security management including people training, adoption of regulatory inputs, identity management, entitlement services, verification services, privacy services, installation of security updates and patches, software/ hardware hardening and server segmentation, configuration management, backup, recovery and restoration, vulnerability monitoring, protection profile	Design, Development and Deployment of: • Resilient systems • Threat scenario simulation, most likely attack forecasting, adversary classification, planning countermeasures, real time attack detection, and response prioritization. • Processes for prioritized countermeasures, information security compliance, disaster and business continuity management, non-repudiation, adoption of emerging solutions and standards, aligning physical and information security solutions, security	Design, Development and Deployment of: • Systems verifying processes for information security management including people training, adoption of regulatory inputs, identity management, entitlement services, verification services, privacy services, installation of security updates and patches, software/ hardware hardening and server segmentation, configuration management, backup, recovery and restoration, vulnerability monitoring, protection profile evaluation, security

	evaluation, security target evaluation, and incidence response. • Processes for risk identification and management, and violation enforcement.	coordination, advisory policies, protecting security functions and operational risk management. • Processes for identifying owners for all the information security related policies and processes. • Streamlined security related process management system. Periodic review and revision of: • Policies and processes for information security management including people training, adoption of regulatory inputs, identity management, entitlement services, verification services, privacy services, installation of security updates and patches, software/ hardware hardening and server segmentation, configuration management, backup, recovery and restoration, vulnerability monitoring, protection profile evaluation, security target evaluation, and incidence. • Processes for identifying owners	target evaluation, and incidence, resilient systems, threat scenario simulation, most likely attack forecasting, adversary classification, planning countermeasures, real time attack detection, response prioritization, processes for prioritized countermeasures, information security compliance, disaster and business continuity management, non-repudiation, adoption of emerging solutions and standards, aligning physical and information security solutions, security coordination, advisory policies, protecting security functions and operational risk management.

		for all the information security related policies and processes	

Table 52: Business opportunities for Infosys in the management maturity domain.

Nature of Business opportunity	Inactive to Reactive	Reactive to Streamlined	Streamlined to Proactive
Consulting	• Security assessment, benchmarking and recommendations for migration. • Risk assumption, limitation and transference, Security controls for information security incidence detection, and recovery, security functional and assurance requirements, Security categorization, requirements and assessment planning.	• Security assessment, benchmarking and recommendations for migration. • Delegation of divisional level accountability for security health, risk avoidance, security control for preventive management, security certification, accreditation, hardware, software and information disposal and disaster management planning. • Study to streamline all security related management components. Periodic review and revision of: • Risk assumption, limitation and transference, Security controls for information security incidence detection, and recovery, security functional and assurance requirements, Security categorization, requirements and	• Security assessment, benchmarking and recommendations for migration. • Risk research, Assured outsourcing and risk reward analyses. Verifiability of: • Risk assumption, limitation and transference, Security controls for information security incidence detection, and recovery, security functional and assurance requirements, Security categorization, requirements and assessment planning. • Delegation of divisional level accountability for security health, risk avoidance, security control for preventive management, security certification, accreditation, hardware, software and information disposal and disaster management planning.

		assessment planning.	• Risk research, Assured outsourcing and risk reward analyses.
IT services		Design, Development and Deployment of: • Disposal management. • Disaster management. • Streamlined security management system.	System for verifying: • Disposal management. • Disaster management.

7. The road ahead

It is important for all concerned to understand that this report and the initial framework is only a little beginning step in a relatively long journey. The desired destination would arrive when a refined version of this framework becomes a standard in the information security end user community. Any new concept needs a bowling alley strategy for adoption. Adoption hurdles have killed many a good technology. INFOSeMM adoption can be achieved through the following efforts.

a. Validating the framework through some pilots.

Infosys can use some of its existing customer base to pilot some projects for the dual purposes of fulfilling customer needs and refining or redesigning the framework based on the feedbacks from the pilots. Our contact with BCM group has given us some pointers. This is a good beginning. It would be important for Infosys to pilot it on its own corporate network. The lessons learnt here can be used to refine the framework and promote it amongst the visionary early adopter client base.

b. Designating owners

Organizational management experience has clearly proven that goods are delivered and responsibility and accountability coexist. It is therefore important to establish the required environment for nurturing this framework to grow into a mature product. So, it is important to identify a team of owners from SET Labs and IBUs who will be responsible for the

- Maintaining the consistency and completeness of the maturity level considerations.
- Generating questionnaires based on the eight sets of maturity considerations.
- Maintaining the maturity level designations for each of the considerations.
- Maintaining the types of client engagements that can use this framework.
- Maintaining the synchronization between the maturity considerations and the INFOSeMM model.

c. Academic validation through publication in

- Information systems conferences and journals.
- Information security management conferences and seminars.
- Management journals addressing information security.

The publication effort in the conferences and seminars can start right away whereas the journal publications would require the results from a couple of pilot studies.

d. Pushing for adoption as a standard

The best approach towards making this a standard would be by getting more and more people accept this and thus making this become a de facto standard.

i. Increased client adoption so that this becomes a de facto standard.

This is best achieved by getting more clients to see value in the maturity framework. This can start once the considerations are firmed up and an internal pilot is done.

ii. Promoting INFOSeMM to relevant standard bodies at the right times.

This effort should begin only after several marquee customers have embraced this framework.

iii. Showcasing INFOSeMM in relevant tradeshows and industry events.

This effort can begin right away.

iv. Writing about INFOSeMM in trade and business magazines.

This effort can also begin right away.

e. Follow on quantitative work.

This Information Security Maturity framework is a qualitative work. We expect companies to be concerned about the cost-benefit and return on investment analysis that will be very quantitative. Such quantitative work will greatly simplify the adoption of this framework.

f. Self-assessment tool

Infosys may wish to evaluate the need to develop a tool that will allow companies to self-evaluate their current state of preparedness for handling information security threats. Such a tool can earn goodwill among current and future customers and lead to follow on engagements.

OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) Framework, Version 1.0

1 Introduction

The Networked Systems Survivability (NSS) Program of the Software Engineering Institute (SEI) has begun developing the Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE^{SM}) framework to describe an information security risk evaluation. OCTAVE defines a set of self-directed activities for organizations to identify and manage their information security risks. Evaluations that are consistent with the OCTAVE framework will be comprehensive and will allow an organization to identify the information assets that are important to its mission, the threats to those assets, and the vulnerabilities that may expose those information assets to the threats. By putting together the information assets, threats, and vulnerabilities, the organization can begin to understand what information is at risk. Once it has a picture of the risks, the organization can design a protection strategy to reduce the overall risk exposure of its information assets.

This document describes the essential components of OCTAVE, focusing on what each process step accomplishes. Issues such as who will perform the steps or how to perform them will be addressed in subsequent publications. By issuing this report, we intend to initiate a discussion of what elements make up a comprehensive information security risk assessment that examines both organizational and technology issues. Over time, as we develop and pilot an evaluation method consistent with the OCTAVE framework, we anticipate that the details described in this report will be modified. When appropriate, we will revise this document and the method to reflect changes based on comments from the community as well as on our field experience.

The current version of OCTAVE comes primarily from the following three sources:

- Information Security Evaluation (ISE). The ISE is an information security vulnerability evaluation developed by the Software Engineering Institute's Networked Systems Survivability Program. It focuses on identifying vulnerabilities in an organization's computing infrastructure. It addresses assets and threats implicitly. OCTAVE developers are incorporating the lessons learned from the development and delivery of the ISE into the OCTAVE framework and method.

- Software risk management expertise. OCTAVE is also incorporating many of the diagnostic techniques and theories developed by the SEI's Risk Program, which focused on identifying risks to software development projects. Many of the principles for OCTAVE's Phase 1 are derived from work that focused on risk management issues facing managers in a software development organization.
- Surveying the current state of the practice in information security risk management. Articles about state-of-the-practice information security assessments were examined prior to the development of OCTAVE. This information was used to determine what is working in the community and where the community could benefit from a self-directed comprehensive information security risk assessment.

1.1 The Need for OCTAVE

Information systems are essential to most organizations today. The integrity, availability, and confidentiality of information are critical to organizations' missions. However, few organizations focus on their most important information assets when they make decisions about protecting their information. For example, a bank might consider its customers' bank records to be one of its important information assets. Likewise, a military organization responsible for deploying troops might consider logistical data to be an important information asset. Most organizations form their protection strategies by focusing solely on infrastructure weaknesses. Those organizations fail to establish the effect of the infrastructure weaknesses on information assets, such as bank records or logistical data.

This leads to a gap between the organization's operational requirements and information technology (IT) requirements. Often, the computing infrastructure is set up without the IT staff having a clear understanding of the organization's mission- or business-related needs. It is not clear if important information is being adequately protected. Likewise, significant effort might be directed toward protecting relatively unimportant information. In these situations, the operational or business units of the organization and the information technology department are not communicating effectively.

Often, information protection decisions are made in an ad hoc manner, based on the IT department's prior experience with vulnerabilities and the threats that they currently know about. Thus, risks tend not to be systematically managed or are managed by the wrong people.

Most current approaches to information-security risk management tend to be incomplete, expert-driven, or both. Most approaches fail to include all the components of information security risk (assets, threats, and vulnerabilities). In these cases, the organization has insufficient data to fully match a protection strategy to its security risks.

Many organizations outsource information security risk assessments because they do not have in-house capability to perform this vital service. They hire experts to perform risk assessments, and the resulting assessment is only as good as the experts who perform it. Often the consumers of such services have no way to understand if the risk assessment performed for them is adequate for their enterprise.

OCTAVE enables organizations to avoid those problems. It defines the essential components of a systematic information-security risk assessment. By following the OCTAVE framework, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information assets. The operational or business units and the departments responsible for the information infrastructure work together to address the information security needs of the enterprise. OCTAVE thus gives the organization a comprehensive, systematic, context-driven approach to managing information-security risks.

1.2 Overview of OCTAVE

OCTAVE examines organizational issues and technology issues to assemble a comprehensive picture of the information security needs of an enterprise. It contains the following phases:

Phase 1, Build Enterprise-Wide Security Requirements

Phase 2, Identify Infrastructure Vulnerabilities

Phase 3, Determine Security Risk Management Strategy

Each phase of OCTAVE is designed to produce meaningful results for the organization.

During Phase 1, information assets and their values, threats to those assets and security requirements are identified using knowledge of the staff from multiple levels within the organization, along with standard catalogs of information. For example, known threat profiles and good organizational and technical practices are used to probe staff members for their knowledge of the organization’s assets, threats, and current protection strategies. This information can then be used to establish the security requirements of the enterprise, which is the goal of the first phase of OCTAVE.

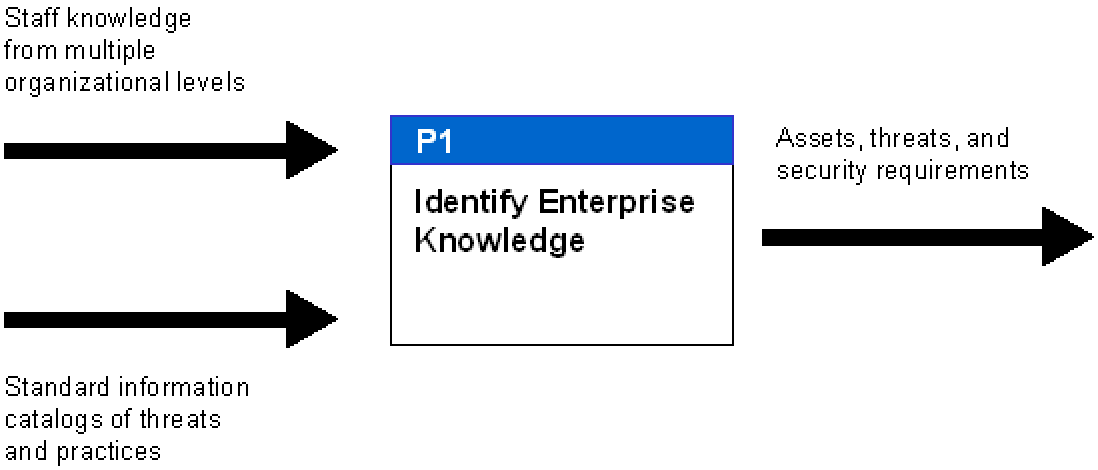
Staff knowledge from multiple organizational levels
P1
Identify Enterprise Knowledge
Assets, threats, and security requirements
Standard information catalogs of threats and practices

Figure 1: OCTAVE Phase 1, Build Enterprise-Wide Security Requirements

Phase 2 of OCTAVE builds on the information captured during Phase 1 by mapping the information assets of the organization to the information infrastructure components (both the physical environment and networked IT environment) to identify the high-priority infrastructure components. Once this is done, an infrastructure vulnerability evaluation is performed to identify vulnerabilities. As in Phase 1, standard catalogs of information are used; for example, standard intrusion scenarios and vulnerability information are used as a basis for the infrastructure vulnerability evaluation. At the conclusion of Phase 2, the organization has identified the high-priority information infrastructure components, missing policies and practices, and vulnerabilities.

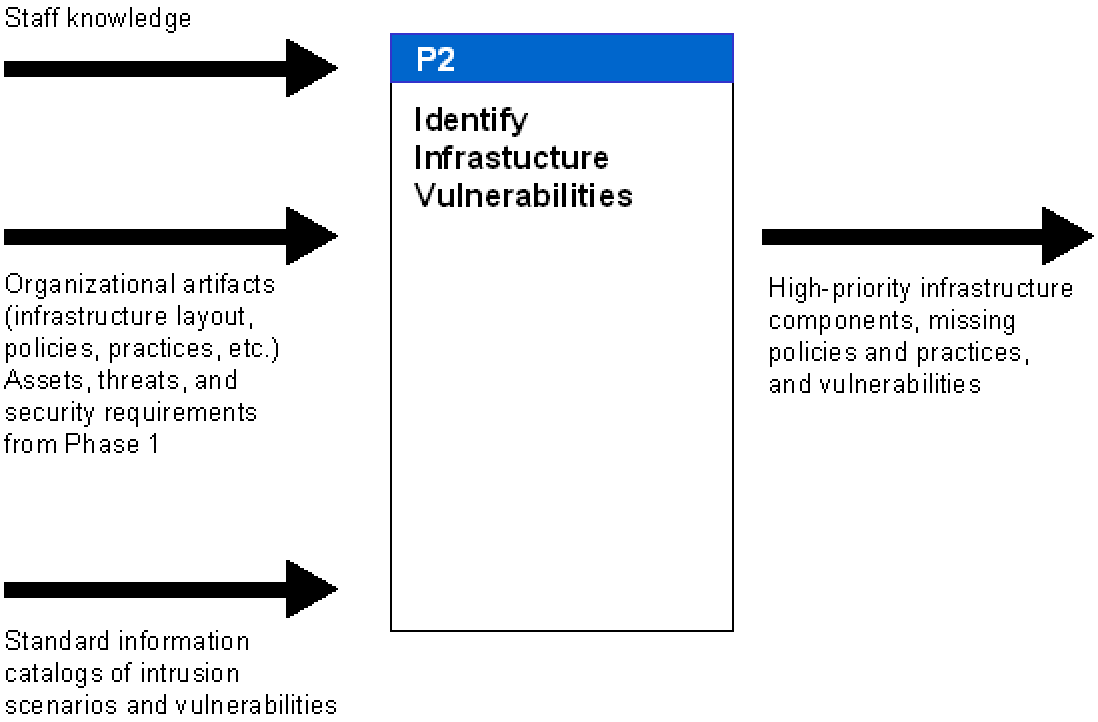
Staff knowledge
P2
Identify Infrastucture Vulnerabilities
Organizational artifacts (infrastructure layout, policies, practices, etc.) Assets, threats, and security requirements from Phase 1
Standard information catalogs of intrusion scenarios and vulnerabilities
High-priority infrastructure components, missing policies and practices, and vulnerabilities

Figure 2: OCTAVE Phase 2, Identify Infrastructure Vulnerabilities

Phase 3 of OCTAVE builds on the information captured during Phases 1 and 2. Risks are identified by analyzing the assets, threats, and vulnerabilities identified in OCTAVE's earlier phases in the context of standard intrusion scenarios. The impact and probability of the risks (also called the risk attributes) are estimated and subsequently used to help prioritize the risks. The prioritized list of risks is used in conjunction with information from the previous phases to develop a protection strategy for the enterprise and to establish a comprehensive plan for managing security risks, which are among the goals of Phase 3.

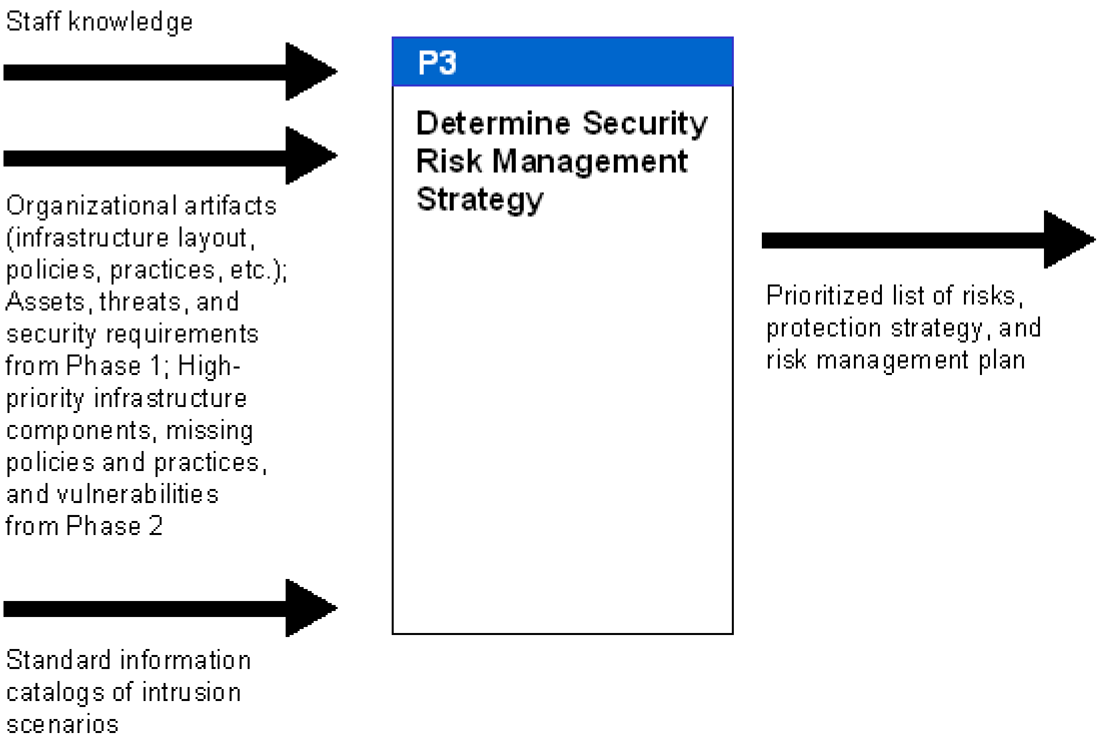
Staff knowledge
Organizational artifacts (infrastructure layout, policies, practices, etc.); Assets, threats, and security requirements from Phase 1; High-priority infrastructure components, missing policies and practices, and vulnerabilities from Phase 2
Standard information catalogs of intrusion scenarios
P3
Determine Security Risk Management Strategy
Prioritized list of risks, protection strategy, and risk management plan

Figure 3: OCTAVE Phase 3, Determine Security Risk Management Strategy

1.3 Example Scenario

To illustrate how using OCTAVE can help an enterprise understand its information security risks, consider the following example. An enterprise with sensitive financial information is interested in understanding and addressing its information security risks. The enterprise's management is concerned that outsiders could have access to financial information that could be used for illegal stock trading. The senior managers decide to perform a security assessment to understand its risk in this area.

An outside consulting firm is hired to evaluate the enterprise's security. The following observations are among those identified by the consultants:

- The enterprise's firewall is functioning correctly—outsiders would have a hard time getting in.
- There are no back doors into the network.
- The number of accounts on most servers is limited.
- Most servers are accessed remotely.
- Authentication is required when users access servers.
- There is one vulnerability: user IDs and passwords travel across the network in clear text.

The consultants failed to develop a picture of the risk facing the enterprise. Consequently, senior managers believed that the financial information was secure, based on the results of the assessment. They felt safe from the threat of outsiders breaking into their network and stealing sensitive financial information. They were not considering other potential threats.

Consider a second evaluation, which is performed by following the OCTAVE framework. Personnel from senior management, middle management, and staff levels participated in the risk evaluation. Phase 1 of OCTAVE was performed to identify assets, threats, and security requirements.

One of the most critical assets identified was the sensitive financial information. If this information were made public, the reputation of the enterprise would suffer and could result in millions of dollars of lost business. In addition, anyone knowing this information could use it to profit illegally by trading stocks. The relative impact of losing the confidentiality of this information was high. Thus, one of the security requirements for the financial information was that it must be confidential.

OCTAVE requires participants to consider a variety of potential threats. (The term "threats" indicates what or whom the assets are being protected from.) Several threats had motivation to possess this information, because the information could be used for financial gain. Furthermore, it was determined that the threats could be insiders or outsiders. One possible means for threats to gain access to the information was via the network, and all employees had access to the network. Technically savvy employees might be able to exploit any vulnerability that might be present.

In addition, the information supplied by staff-level employees indicated that there was some dissatisfaction among some of the technical employees in the company. Thus, disgruntled insiders might have both the motive and the means to steal the information.

Next, Phase 2 of OCTAVE was performed to identify infrastructure vulnerabilities. First, the important infrastructure components were identified through an examination of the layout of the physical and IT infrastructures. Because sensitive financial information was an important information asset, the server that contained the database with that information was identified as a high-priority component. A vulnerability evaluation for the server was performed.

The vulnerability evaluation indicated the following:

- The number of accounts on the server holding the sensitive information is limited.
- The server is accessed remotely.
- Authentication is required when a user accesses the server.
- There was one major vulnerability: user IDs and passwords travel across the network in clear text.

Phase 3 of OCTAVE calls for an analysis of the asset, threat, and vulnerability information identified during Phases 1 and 2, in the context of intrusion scenarios to identify the organization's risks. For example, the following intrusion scenario can be built using the information in this example:

> *A technically savvy, disgruntled insider uses a network sniffer to steal passwords to the server containing the sensitive database. As soon as a password is known, the insider can access the sensitive information and use it for personal gain or make it public.*
>
> *The likelihood of such an attack was judged to be moderate to high. The impact would be high in terms of damage to the company's reputation. This was judged to be a big risk to the enterprise.*

The senior managers understood the nature of this risk. They understood that it was possible for a sufficiently motivated insider to steal sensitive financial information and use it for profit. This was only one of many such risks to be identified using OCTAVE. The enterprise staff was now ready to start developing a strategy to protect the sensitive financial information as well as other important assets.

By performing a comprehensive risk assessment that considers asset, threat, and vulnerability information and puts it into the context of the enterprise, the risks facing the enterprise can be identified. In addition, personnel from all levels can understand risks when they are put into the context of the enterprise, and can make sensible decisions concerning a protection strategy.

1.4 Report Overview

In the rest of this report, OCTAVE will be outlined in detail. We will describe each of the three phases of OCTAVE and the multiple processes within each phase. For each OCTAVE process, we include the following:

- process activities—a high-level description of what happens at each step of the process. Included with the description of each activity is a description of the inputs and outputs of each process.
- process diagram—a data-flow diagram showing the inputs and outputs of the process

Following the phase and process descriptions are higher-level views of OCTAVE. Section 5 concisely summarizes OCTAVE goals and processes. The appendix provides a flowchart of the OCTAVE method.

[1] Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

Related resources

The INFOSeMM framework working document (in EXCEL).

IT Security Maturity Model assessment document (in EXCEL).

Presentation on INFOSeMM (in Powerpoint)