Information Security Management at HDFC Bank: Contribution of Seven Enablers

By Vishal Salvi, CISM, and Avinash W. Kadam, CISA, CISM, CGEIT, CRISC, CBCP, CISSP, CSSLP

HDFC Bank was incorporated in August 1994 and currently has a nationwide network of 3,062 branches and 10,743 automated teller machines (ATMs) in 1,568 Indian towns and cities.

HDFC Bank operates in a highly automated environment in terms of IT and communication systems. All of the bank’s branches have online connectivity, which enables the bank to offer speedy funds transfer facilities to its customers. Multi-branch access is also provided to retail customers through the branch network and ATMs.

The bank has prioritised its engagement in technology and the Internet as one of its key goals and has made significant progress in web-enabling its core businesses. In each of its businesses, the bank has succeeded in leveraging its market position, expertise and technology to create a competitive advantage and to build market share.

Use of COBIT

As an early adopter of COBIT 4.1, HDFC Bank’s IT governance journey started almost six years ago, when COBIT 4.1 was just introduced. Almost all of the 34 IT processes defined in COBIT 4.1 were adopted by the bank.

Following COBIT 5’s introduction in April 2012, HDFC Bank took some time to consider a migration. Because the bank has successfully implemented COBIT 4.1 to great benefit, it will not immediately migrate to COBIT 5. However, the seven enablers introduced by COBIT 5 were intuitively adopted by HDFC Bank even before these were popularised in COBIT 5.

COBIT 5 describes seven enablers, which are factors that, individually and collectively, influence whether something will work—in this case, governance and management of enterprise IT (GEIT):

1. **Principles, policies and frameworks** are the vehicles to translate a desired behaviour into practical guidance for day-to-day management.
2. **Processes** describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
3. **Organisational structures** are the key decision-making entities in an enterprise.
4. **Culture, ethics and behaviour** of individuals and the enterprise are often underestimated as a success factor in governance and management activities.
5. **Information** is pervasive throughout any organisation and includes all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is often the key product of the enterprise.
6. **Services, infrastructure and applications** include the infrastructure, technology and applications that provide the enterprise with IT processing and services.
7. **People, skills and competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

This article describes how these seven enablers have contributed towards better information security management at HDFC Bank.

Organisational Structures

Organisational structures are the key decision-making entities in an enterprise.

Information security at HDFC Bank is driven by its information security group (ISG). The group is headed by the chief information security officer (CISO), who reports to the executive director of the bank. The ISG is primarily responsible for identifying, assessing and proposing mitigation for every information-security-related risk. This responsibility is carried out by interacting with various committees and stakeholders and preparing plans, proposals, policies, procedures and guidelines. The implementation of these is assigned to the implementation teams across the bank.
The governance framework at HDFC Bank is driven by a number of top-level committees (figure 1). The importance given to information security is evident from the number of top-level committees that have information security on their agenda.

Roles and responsibilities for the ISG have been well defined through a RACI chart (figure 2). One of the main points to be noted is that, although the responsibility for information security management is with the ISG, the accountability is squarely with the function heads. Similarly, although the ISG is accountable for the risk assessment definition, function heads are accountable for risk assessment execution. This segregation of responsibility and accountability creates ownership of risk mitigation and information security tasks.

security management with the function heads.

The overall framework for governance to implementation is provided in **Figure 3**.

The 21 components are constantly monitored for maturity level. The assignment of work to the ISG team members are based on these controls.

**Principles, Policies and Frameworks**

Principles, policies and frameworks are the vehicles to translate the desired behaviour into practical guidance for day-to-day management.

HDFC Bank has created a comprehensive policy document of around 100 pages. The current version is 3.x, and it is being revised to version 4.0. This document covers the 11 information security domains as specified in ISO 27001 in a platform- and technology-agnostic manner. It is modeled on Information Security Forum (ISF)’s **Standard of Good Practices**.

Since the bank uses 30 to 40 different technologies, there are more detailed policies created for each technology. These are fine-grained technology-specific policies for reference by the technical team responsible for implementing these technologies.

These policies are further subdivided into records for mapping against various authoritative standards/frameworks, such as ISO 27001, COBIT and Reserve Bank of India (RBI) guidelines. These records are input into a governance, risk and compliance (GRC) tool that provides a unified control framework (UCF). This helps to identify, in an automated fashion, the compliance level achieved. The tool provides almost 40 authoritative sources that are already mapped through the UCF. Thus, compliance with any source can be easily found.

The ISG team uses the Factored Analysis of Information Risk (FAIR) methodology for computing probable risk by capturing threat event frequency and loss event frequency, giving appropriate weight to each factor, and deriving the risk rankings for prioritising and decision making. The ISG team also reviewed ISO 27005 and created a sound approach to risk management with the help of these standards.

A short version of the policy document has been created as a 20-page user guide supported by a list of top 10 rules for information security.

There are a number of vendors providing services to HDFC Bank. The supply chain security is assured by regular third-party reviews of vendors, which are performed by external audit firms.

HDFC Bank is certified for ISO 27001 and BS 25999, is planning to achieve the ISO 22301 certificate, and has achieved 92 percent compliance with the RBI guidelines.
The ISG team is currently focused on creating a sound incident management system; providing adequate data protection; ensuring appropriate implementation of bring your own device (BYOD); and detecting, containing and removing advanced persistent threats in a timely fashion.

**Processes**

Processes describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals. The ISG follows an information security process model based on 21 components:

1. Application security
2. Cryptography
3. Monitoring
4. Incident management
5. Online banking security
6. Malware management
7. Data protection
8. Secure software development life cycle
9. Vendor (third-party) management
10. Business continuity planning
11. Privacy
12. Identity and access management
13. Risk management
14. Physical security
15. Awareness
16. Governance
17. Policy
18. Asset life cycle management
19. Accountability and ownership
20. System configuration
21. Network security

The information security planning, designing, deployment and monitoring is done for these individual components. This approach keeps the teams focused. The policies, procedure, guidelines, standards, technologies and tools are built for these components. This approach provides granularity in managing each focus area and also leads to defense-in-depth architecture.

Each of the components contributes to building the control standards and control procedures that satisfy high-level policy requirements. This is a bottom-up approach which serves to mitigate the top-level security concerns for business processes by providing adequate security for the assets used by these processes.

The work of mapping all business processes with assets is currently being carried out. The business processes are being ranked based on the criticality and impact they may have on the business. If one asset, e.g., a server, is hosting multiple IT processes supporting multiple business processes, it gets the ranking attributed to the most critical business process.

The approach followed by the HDFC Bank ISG is closely aligned with COBIT 5’s goals cascade (figure 4).

---

**Figure 4—COBIT 5 Goals Cascade**

Stakeholder drivers identified by HDFC Bank are shown in **figure 5**.

**Figure 5—HDFC Bank Stakeholder Drivers**

- Legal & Regulatory
- Socio-cultural
- Threat Landscape
- Government
- Technology

- Payment Cards Industry Data Security Standard (PCI DSS)
- RBI Regulations for Cyber Security Controls – April 2011
- Indian Privacy Law – WIP
- IDRBT Information Security Framework
- Hacktivism
- Cybercrime
- Cyberattacks
- Advance Persistent Threats
- Cyberespionage
- Information Leakage
- Mobile Malware
- Virtualisation
- Cloud Computing
- Big Data
- IP V6
- UID
- NAT-GRID
- E-governance Projects
- Cybersecurity Policy for India
- Creation of Sectorial CERTS


**Information Security Maturity Levels**

ISG has developed an information security maturity model. The model has defined five levels of maturity as shown in **figure 6**.

**Figure 6—Information Security Maturity Model**

<table>
<thead>
<tr>
<th>Column1</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>No policy</td>
<td>Limited policy</td>
<td>Comprehensive policy defined and published</td>
<td>Policy published and implemented consistently</td>
<td>Continuous review and improvement of the policy</td>
</tr>
<tr>
<td>Roles and responsibilities</td>
<td>No defined roles and responsibilities</td>
<td>Roles somewhat defined</td>
<td>Clear roles and responsibilities defined</td>
<td>Roles and responsibilities defined and executed</td>
<td>Roles and responsibilities reviewed on ongoing basis</td>
</tr>
<tr>
<td>Automation</td>
<td>Manual</td>
<td>Semi-automated</td>
<td>Automated</td>
<td>Automated and fully operational</td>
<td>Constant upgrade of automation</td>
</tr>
<tr>
<td>Scope</td>
<td>Not implemented</td>
<td>Limited coverage</td>
<td>Critical assets</td>
<td>Complete</td>
<td>Regular review of scope to ensure 100% coverage</td>
</tr>
<tr>
<td>Effectiveness</td>
<td>NA</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very high</td>
</tr>
<tr>
<td>Incident Management</td>
<td>No tracking</td>
<td>Limited visibility</td>
<td>Critical incidents tracked</td>
<td>All incidents tracked and closed</td>
<td>RCA done for all incidents and remediated</td>
</tr>
<tr>
<td>Measurement</td>
<td>No measurement</td>
<td>Limited measurement</td>
<td>Comprehensive measurements defined</td>
<td>Measured and reviewed on a regular basis</td>
<td>Measurement criteria reviewed regularly</td>
</tr>
<tr>
<td>Reporting</td>
<td>No reporting</td>
<td>Limited reporting</td>
<td>Reporting defined</td>
<td>Reports sent to senior management and reviewed</td>
<td>Reporting requirements regularly reviewed and updated</td>
</tr>
</tbody>
</table>

ISG has defined eight desirable attributes for information security components. These are listed in column 1. Requirements for achieving each level for an attribute have been defined in the subsequent columns. For example, the policy attribute is at level 1 if there is no policy defined for a particular component, and it is at level 5, i.e., optimised, if there is continuous review and improvement of the policy.

Tracking of each of the 21 components is based on this model. The maturity model has been successfully used by HDFC Bank to build a sense of benchmarking within the organisation. It helps in finding areas for improvement. These evaluation exercises are done in a workshop mode. There is a healthy two-way communication leading to a sense of participation and clarity about the strategy and vision of the enterprise. The model is strictly used for internal gap analysis and for identifying areas for improvement. It is not meant for use to provide assurance to a third party.

The above maturity model was created by the ISG to meet its unique needs for defining specific improvement plans. This maturity model is loosely based on the maturity model defined in COBIT 4.1. One of the criticisms of the COBIT 4.1 maturity model was that the criteria for levels are subjective. HDFC Bank is now considering mapping the current processes with the COBIT 5 Process Assessment Model (PAM), which is based on ISO 15504.

Services, Infrastructure and Applications
Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with IT processing and services.

HDFC Bank uses almost 40 different technologies. Various services, infrastructure and applications are built around these technologies. As described under the processes enabler, each of these services is mapped to the information security maturity level. A continuous updating of the maturity level against attributes such as automation, effectiveness, incident management and measurement ensures that these services are monitored very closely. All projects for improvement of the services are based on the maturity level aimed at the particular service.

Information
Information is pervasive throughout any organisation and includes all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is often the key product of the enterprise.

Reliable information for security management is a key factor. Information in terms of strategy, budget, plan and policies is regularly presented through board papers. Information security requirements are captured through a risk acceptance form (RAF) and are reviewed at the information security risk management committee (ISRMC). The ISG also prepares various information security review reports, including audit findings, maturity reports, threat analyses, vulnerability assessment reports, information risk registers, breaches and loss reports, and information security incident and problem reports.

The maturity model provides additional inputs for good quality information. Various information security metrics and measurements have been created based on the ISO 27004 framework and are presented as a dashboard. Currently, work is in progress to implement an IT GRC tool to capture all the information at the source and demonstrate compliance against numerous requirements, including RBI guidelines, PCI DSS and Basel II. The tool also provides mapping of various controls from COBIT 4.1.

People, Skills and Competencies
People, skills and competencies are linked to people and are required for successful completion of all activities, for making correct decisions and taking corrective actions.

HDFC Bank has deployed a number of techniques to create awareness about security and to build appropriate skills and competencies. Following is a list of some of the initiatives:

- **Information security movie**—A 20-minute movie was created and presented with all the trappings of a real movie theatre experience (e.g., tickets, popcorn). The movie has proven extremely popular, and so far 40,000 employees have seen it. Every training programme begins with this movie.

- **Information security cartoon strip**—A cartoon strip was created with two characters, one named Sloppy and the other Sly. Their exploits entertain the readers and also carry a very powerful security message. This cartoon strip is now planned to be printed in a calendar format.

- **Security net**—The security net (an intranet) houses all relevant material, such as policies, standards, guidelines, contact
lists, business continuity plans and approach notes.

- **Email and picture campaign**—Regular emails are sent cautioning everyone about being alert, e.g., a reminder about avoiding phishing emails is sent after any successful phishing attempt.

- **Ten security commandments**—The user policy document has been summarised into key information security rules that are easy to read and remember (figure 7).

- **Security First course**—All employees have to undertake this one-hour course every two years. Taking the examination and obtaining passing marks is mandatory. A certificate is issued to all successful candidates. Apart from the certificate, the star performers are also recognized through global mailers sent to all the bank’s employees as well as monetary rewards.

- **One-day workshop**—A one-day workshop is conducted periodically for senior management at which the CISO explains the importance of information security for the bank and the specific measures deployed for its implementation.

**Culture, Ethics and Behaviour**

Culture, ethics and behaviour of individuals and the enterprise are often underestimated as a success factor in governance and management activities. Nonetheless, they are important contributors to the success of an enterprise.

COBIT 5 has identified eight types of behaviours that contribute to building security culture in an organisation. Various initiatives taken by HDFC Bank have led to creating the right type of security behaviours. HDFC Bank has used multiple channels of communication, enforcement, clear policies, rules and norms. Secure behaviour is also encouraged through recognition, e.g., a security certificate, and strong messages to defaulters. Secure behaviour is strongly influenced through raising awareness.

The eight types of behaviour are reproduced here for reference along with the specific measures adopted by HDFC Bank to embed these behaviours into the daily practice of bank employees:

- **Information security is practiced in daily operations.** HDFC Bank management has conveyed its expectations of employees by stressing the principle of zero tolerance for unacceptable behaviour relating to information security, rewarding good behaviour, recognising and rewarding people for good work towards risk management, and constantly reminding everyone through the tagline “Security is incomplete without U.” This has ensured that information security is practiced in daily operation.

- **People respect the importance of information security policies and principles.** The security culture has been built over time through constant efforts in creating awareness. Employees now understand the importance of information security and take security initiatives seriously. Audit has also played an important role in enforcing various security policies and principles.

- **People are provided with sufficient and detailed information security guidance and are encouraged to participate**
in and challenge the current information security situation. HDFC Bank believes in engaging all stakeholders in the security effort. Introduction of any new process involves ensuring open interaction with all the affected parties. The issues are discussed in workshops and buy-in is achieved through two-way dialogue—allowing everyone to clarify any doubts they may have. Extensive training is provided for every new information security initiative, not only to the information security group but to all stakeholders.

- **Everyone is accountable for the protection of information within the enterprise.** The information security group is responsible for identifying and managing the risk whereas the business heads are held ultimately accountable. This has been clearly documented in the RACI chart discussed earlier. This makes all the stakeholders feel responsible as well as accountable for protection of information within the enterprise.

- **Stakeholders are aware of how to identify and respond to threats to the enterprise.** Threat identification is part of the training provided to stakeholders. Stakeholders are encouraged to report incidents, e.g., send an email to the ISG about any spam or phishing email received. The response received by the ISG on a day-to-day basis shows the keen awareness of everyone to identify and report incidences.

- **Management proactively supports and anticipates new information security innovations and communicates this to the enterprise.** The enterprise is receptive to account for and deal with new information security challenges. ISG is constantly engaged in introducing innovations to deal with information security challenges. There is full management support to interact with industry and share knowledge and experience with a larger audience as well as learn from others. This case study is an example of this openness.

- **Business management engages in continuous cross-functional collaboration to allow efficient and effective information security programmes.** The structure of various committees is an example of continuous cross-functional collaboration. Making information security independent of the IT function has provided a much broader reach and direct access to various business groups across the organisation.

- **Executive management recognises the business value of information security.** The CISO works at a strategic level, reporting to a senior person in the bank. This has empowered the CISO to drive various information security initiatives with a great amount of freedom. This is a good indication of management’s recognition of the business value of information security.

### Leadership as an Influencing Factor

In addition, the leadership in HDFC Bank plays a prominent role in building the security culture.

Active participation by executive management and business unit management in the various top-level committees where information security is an important agenda item demonstrates the commitment at the top. Participation by leadership in business continuity planning exercises to discuss various disaster scenarios also shows deep involvement.

### Vishal Salvi, CISM

Has more than 20 years of industry experience, having worked at Crompton Greaves, Development Credit Bank, Global Trust Bank and Standard Chartered Bank before taking on his current role as chief information security officer and senior vice president at HDFC Bank. At HDFC Bank, he heads the information security group and is responsible to provide leadership to the development and implementation of the information security program across the bank.

### Avinash W. Kadam, CISA, CISM, CGEIT, CRISC, CBCP, CISSP, CSSLP

Is a leading authority on information security. He has four decades of experience in IT management, information systems audit, and information security consulting and training. He is currently advisor to ISACA’s India Task Force. Previously, Kadam served as an ISACA international vice president from 2006 to 2008 and president of the ISACA Mumbai Chapter from 1998-2000. He is the recipient of ISACA’s 2005 Harold Weiss Award.

©2013 ISACA. All rights reserved.