In today’s economy, outsourcing is an essential business strategy. Outsourcing helps enterprises save money by leveraging the economies of scale realized by the outsourcing suppliers. When effectively managed, it also helps relieve enterprises from the problems of manpower constraints, skills shortages and operating efficiencies.

In pursuit of benefits such as less expensive labor, availability of a large pool of talented resources and faster time to market, enterprises utilize offshore service providers from countries such as India and China. Many enterprises take to offshore outsourcing end-to-end, engage the service provider as a partner, and strive for achieving performance improvements, productivity gains and continuous innovations over time.

This offshore outsourcing, however, is not without risks and challenges. Some of the key challenges in this scenario are:

• Multiple organizations and their security systems are now involved, making security system design and ongoing operations complex.
• Since different countries are involved, different laws and regulations are applicable. Careful management is required to ensure that legal and regulatory compliance is achieved.
• Offshore service providers usually cater to the needs of many enterprises (clients), and this results in additional complexities.
• Priorities and standards of the service provider for business continuity and disaster recovery preparedness can be different from those of the client on many occasions, and this could result in complications.
• Work is conducted “out of sight” at remote locations, and this results in an apparent loss of control unless suitable ways are implemented to ensure ongoing control.

While experienced companies have been outsourcing IT development and business back-office functions for many years, inexperienced organizations may be rushing to jump on the offshore outsourcing bandwagon too prematurely. The importance of proper offshore outsourcing plans and risk management is evident from a recent study published by DiamondCluster International, a US-based global management consulting firm. DiamondCluster found that the number of buyers prematurely terminating an outsourcing relationship has doubled to 51 percent, while the number of buyers satisfied with their offshore providers has decreased from 79 percent to 62 percent.¹ ²

Effective information security management becomes crucial in this scenario. This article describes a framework that can be used for measuring and reporting the performance of information security in such an instance.

**What Is an Information Security Program?**

An information security program involves the overall combination of technical, operational and procedural measures and management structures implemented to provide the confidentiality, integrity and availability of information based on business requirements and risk analysis.¹ An information security program depends heavily on the processes established as a result of information security governance efforts in the organization.

Information security governance aims to develop a system through which organizations are directed and controlled, and integrate security planning in the larger context of IT and business planning. Security governance involves the development and integration of a management structure and organization with reporting processes that encompass all aspects of a successful security program and provide assurance to businesses that risks are defined and appropriately managed.¹ Information security governance is essentially the responsibility of top management.

Effective information security governance and information security programs involve a wide range of activities. Some of the major categories of these activities are:

• Issue and regularly update policies, procedures, standards and guidelines
• Actively monitor for compliance, risks and changes to the context
• Conduct intrusion testing with appropriate detail and regularity
• Design appropriate security defenses and periodically enhance these defenses
• Effectively manage security to ensure timely action and create business-relevant value

**Figure 1** illustrates the activities that help ensure effective information security governance.
In every organization, information security cuts across the entire organization and requires involvement of employees at all levels. In the scenario of offshore outsourcing, information security processes span across the organizations in multiple countries (with the offshore center forming an extended part of the outsourcing organization), requiring effective orchestration of the activities across the extended organization.

**Offshore Outsourcing and the Information Security Program**

Enterprises typically pursue outsourcing after establishing a process and carrying out a number of activities. These activities can be grouped under:

- **Preoutsourcing activities**—These are carried out by the organization before an outsourcing contract is established with the service provider. Examples include:
  - Carrying out a due diligence exercise to select a service provider
  - Assessing security risks involved
  - Assessing security competency of the service provider
  - Establishing security systems and processes
- **During outsourcing**—These activities are to be carried out during the award of the contract and throughout the duration of the contract. Examples include:
  - Establishing the contractual obligations and setting up the master service agreement elaborating the service level, security and operational requirements, review and audit mechanisms, and various contractual processes
  - Assessing the continual performance of the service provider
  - Establishing the information security governance of the outsourcing, covering the structure, roles and responsibilities to manage the various aspects of the engagement, including information security. Reporting responsibilities, methods and associated aspects are also established.
  - Continually enhancing the information security programs
- **Postoutsourcing activities**—These refer to the activities that the organization is to perform upon termination of the outsourcing contract.

Many service providers establish comprehensive security management systems complying with standards such as ISO 17799 (BS 7799), and they also pursue certification to enhance the information security. Many service providers pursue ITIL (BS 15000/ISO 20000) to enhance the service orientation of the IT services. Multiyear contracts are common in these outsourcing engagements, and the parties establish long-term contracts.

The enterprise and the outsourcing service provider approach the engagement as partners and establish systems and processes for the success of the relationship. In particular, the parties work to align the security systems at the offshore center in line with the security systems and requirements of the client.

**Framework for Metrics and Reporting**

The proposed framework aims at security performance measurement and feedback at various levels (strategic, tactical and operational) at the service provider organization and connecting the client (outsourcing its requirements) with a focus on the offshore services.

**Elements of the Framework**

The framework involves the following setup:

- Metrics are worked out for the various performance aspects and are monitored on an ongoing basis using the systems and processes at the offshore service provider end. They are validated as required.
- Performance measurement scorecards are derived and used to track performance at the following levels:
  - Strategic or business level
  - Tactical or IT/IS level
  - Operational or IT process level
- A dashboard is maintained for the management by the service provider.
- A dashboard is maintained for management of the client.

The reporting system is established for appropriate feedback to concerned personnel in both organizations and also for tracking these actions.

Along with the dashboards, the scorecards support the overall management structure, organization and responsibilities that are defined at both the service provider and the client, resulting in greater alignment, better cooperation and more timely action.

**KGI s and KPIs**

The scorecards are derived using key goal indicators (KGIs) and key performance indicators (KPIs).

According to the IT Governance Institute’s *Management Guidelines*, a KGI is defined as “a measure of what has to be accomplished.” A KPI is “the measure of how well the process is performing.”

KGIs and KPIs at the various levels are interrelated. Business KGIs are dependent on the KPIs at the business level.
and, in turn, on KGIs and KPIs at the lower level. Figure 2 shows this hierarchy.

Typical business-level KGIs at the offshore center include:
• Average cost of security incident during a period
• Cost incurred to deal with known threats
• Downtime of critical operations due to security incident
• Number of projects stopped or delayed due to security incident/issues
• Speed of dealing with a new threat
• Time taken to enroll an agent/employee
• Number of reported security incidents
• Number of incidents that are handled without resulting in a crisis
• Time taken to implement a regulatory requirement
• Availability of an information security management system (ISMS) that meets the requirements of the client and is suitably certified/accredited

This list is partial and suggestive only; actual indicators will depend on the scenario and priorities. The organizations will have to decide on KGIs in the context of their priorities.

It may also be noted that business-level KPIs, in most cases, are the same as the tactical-level KGIs.

Typical tactical-level KGIs at the offshore center include:
• Percentage of assets covered by systematic risk assessments
• Number of vacancies in the security roles required for the ISMS
• Time taken to grant, change and remove access privileges
• Percentage of agents covered by an effective security awareness program
• Number of security access violations
• Number of emergency changes
• Number of security incidents involving malicious code
• Number of systems where security requirements are not met
• Average turnaround time of incidents
• Number of pending actions to meet response and recovery requirements
• Number of scheduled internal audits not completed
• Number of scheduled penetration tests not completed

This list is also partial and suggestive; actual indicators will depend on the scenario and priorities of the organization.

Typical operational-level KGIs are:
• Number of obsolete accounts
• Number of unauthorized IP addresses and ports
• Number of cryptographic keys compromised and revoked
• Number of access rights revoked, reset or changed
• Number of security awareness training programs for agents/employees
• Percentage of agents/employees covered by fire/evacuation drill
• Percentage of agents/employees covered by business continuity planning (BCP) training
• Number of overdue actions arising from audit reports
• Number of changes not carried out as per change control procedures

Again, this list is partial and suggestive; actual indicators will depend on the scenario and priorities of the organization.

Typical operational-level KPIs are:
• Number of violations of segregation of duties
• Number of users who do not comply with password standards
• Percentage of suspected and actual access violations
• Percentage of critical assets covered by internal/external penetration tests
• Number of computers with patches behind the service level agreement (SLA)
• Number of outdated policies, procedures, standards and guidelines
• Number of internal audits scheduled
• Number of independent reviews scheduled
• Percentage of agents/employees trained on information security policies and procedures as part of induction
• Number of corrective/preventive actions taken based on analysis of logs
• Number of changes not carried out as per change control procedure
The enterprise buying the services considers its own balanced scorecard (implemented for its business) during the process. This reflects the performance requirement on the following perspectives:

- Financial perspective
- Customer perspective
- Internal process perspective
- Learning and growth perspective

The internal process perspective covers the various internal processes and the requirements of security, effectiveness, efficiency, and compliance with laws and regulations.

Reporting on the balanced scorecard results in tracking the KPIs and KGIs and in overall interpretations under the four perspectives. Acceptable levels can be predefined to identify the status as green, amber or red for the purpose of reporting. The balanced scorecard provides the strategic and top-down perspective to the entire measurement and management of the partner.

Reporting on the balanced scorecard can be done on a quarterly basis to start with, and the results can be used for periodic performance reviews of the respective management teams.

---

**Figure 3—Reporting Framework Balanced Scorecard Report for the Program**

- Establish the Relationship/Annual Reviews
- Establish and Enhance the Balanced Scorecard
- Identify and Enhance KPIs KGIs for All Levels
- Establish the Reporting and Reviewing Processes, Roles and Responsibilities
- Dashboard of Client Management
- Dashboard of Partner Management
- Operational-level Scorecard Reports
- Tactical-level Scorecard Reports
- Balanced Scorecard Reports
- Feedback

Operational/Process
Tactical/IS/IT
Strategic/Business

Teams Responsible for Reporting
teams and form part of the strategic reports. As the process settles down, the results can be tracked on a monthly basis.

Figure 3 shows the overall framework. Figure 4 shows a typical balanced scorecard report for the program. A tactical-level scorecard is a summary report derived from the tracking of KGIIs and KPIs at the tactical level. Since KPIs at the tactical level and KGIIs at the operational level are the same in most cases, the performance of KPIs is derived from the performance scorecard on KGIIs at the operational level.

As organizations set up ISMSs based on frameworks such as ISO 17799 and Control Objectives for Information and related Technology (COBIT), these KGIIs can be chosen in line with these frameworks, readily summarized into the control domains and presented.

Acceptable levels of the indicators are predefined and are used to show the overall status as green, amber or red. This can be reported on a monthly basis to start with and can be used as the report for status reporting at the tactical level. As the process settles down, it can be reported on a weekly basis.

Figure 5 depicts an example of a typical tactical-level scorecard for the program.

Performance at the operational level is tracked using the operational-level scorecard. The KPIs and KGIIs for this purpose will help in tracking the operational purposes. Since substantial work at operational level is in respect of compliance tracking against implemented systems, measures are predominantly in the nature of compliance tracking.

Acceptable levels of the indicators are predefined and are used to show the overall status as green, amber or red for each group of the KGIIs and KPIs.

Compliance is tracked by reports generated on a more frequent basis (usually weekly to begin with and then daily, if required). Figure 6 shows the operational-level scorecard tracking the KGIIs, and figure 7 shows the operational-level scorecard for tracking the KPIs.

The service provider’s management maintains a dashboard where the balanced scorecard, tactical-level scorecard and operational-level scorecard are displayed. Actions initiated/taken to correct or prevent issues are also shown on the dashboard. This enables appropriate oversight by the service provider’s management.

The client also maintains a dashboard that is linked to the dashboard of the service provider. Using this dashboard, the client’s management tracks and takes any corrective actions required. The dashboard can even be maintained as part of the service provider’s automated system, which can provide a dashboard view relevant to the client and enable interaction by the client.
Benefits of the Reporting Framework

The reporting framework has several benefits, including:
• The framework helps integrate the various information security mechanisms across the partners that are normally used for monitoring and managing an outsourcing engagement.
• The framework enables an effective feedback system, integrating the reports and actions at various levels with respect to information security. This, in effect, results in a consistent and closed-loop process and engages the process owners and key personnel of both organizations.
• This framework can facilitate the efforts toward identifying and taking up requirements in a proactive manner and with a more holistic perspective.
• The tactical-level scorecard can be enhanced to include further tactical parameters that need to be monitored in addition to the control objectives; such additions can be periodically checked with penetration testing, audits and reviews.
• If an enterprise is outsourcing to multiple service providers (multisourcing), this framework can be extended to cover the various relationships, enhancing the success of information security performance outsourcing.5, 6
• If a service provider is serving multiple clients, implementing this reporting framework can support the efforts of the service provider to have an information security program appropriate to each client.
• The framework can help in looking at performance as having more than the financial or cost dimension. A broader perspective has important ramifications and helps in achieving outcomes that lead to more satisfying relationships over a period of time. In particular, the learning and growth perspective emphasized in the balanced scorecard (and at the strategic level) leads to innovations in the overall information security program.
• The framework can help manage a relationship with many levels of interactions, ongoing tracking and timely reviews, motivating talent and performance, and building trust. Automation of the reporting and feedback system helps set up a seamless team across the organizations.
• The framework can enable more consistent incorporation of changes, laws and regulations, thereby helping to improve compliance.
• While each of the organizations can implement its own internal control system according to standards and frameworks decided by business priorities, this reporting framework essentially focuses on information security performance in outsourcing and can help in meeting the information security program requirements of the client.

<table>
<thead>
<tr>
<th>No</th>
<th>Control/KGI</th>
<th>Target</th>
<th>Actual</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Percentage of assets covered by systematic risk assessments</td>
<td>&gt;99</td>
<td>98</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Number of personnel vacancies in the security roles required for ISMS</td>
<td>Nil</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Time taken to grant, change and remove access privileges</td>
<td>Max. 2 hours</td>
<td>1.5 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Percentage of agents covered by an effective security awareness program</td>
<td>100%</td>
<td>99%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Number of security access violations</td>
<td>&lt;2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Number of emergency changes</td>
<td>&lt;5</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Number of security incidents involving malicious code</td>
<td>Max. 2</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Number of systems where security requirements are not met</td>
<td>Max. 2</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Average turnaround time of incidents</td>
<td>Max. 2 hours</td>
<td>2 hours 25 minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Number of pending actions to meet response and recovery requirements</td>
<td>Max. 5</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Number of scheduled internal audits not done</td>
<td>Max. 1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Number of scheduled penetration tests not done</td>
<td>Max. 1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Number of overdue actions arising out of audit reports</td>
<td>Max. 5</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Number of changes not carried out as per change control procedure</td>
<td>Max. 1</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Target and actual amounts are hypothetical figures for the purpose of this example. Categorization into green, amber and red is done on a predefined basis.

Figure 5—Example of a Tactical-level Scorecard
Implementing the Reporting Framework

This reporting framework is ideally established as the relationship is formed. If the relationship already exists, implementation can be done as a part of a major review, e.g., annual review/goal-setting exercise.

Starting with the balanced scorecard, the KPIs and KGIs are to be firmed up for the various levels, and the individual scorecards are to be finalized and implemented. Along with these, dashboards are to be set up for the management of the service provider and the client.

Effective implementation of this framework requires extensive collaboration and automation of the processes. The overall implementation results in a performance system covering all levels of the relationship and can prove to be a distinct advantage in managing the risks involved in outsourcing. These are among the aspects that justify the investment in setting up a reporting framework for the engagement. With an increasing number of software solutions available for scorecard development and dashboards, these are more readily possible than in the past.

In summary, the framework supports efforts in establishing accountability at the various levels of the organizations, facilitates continuous monitoring and joint decision making, and engages the stakeholders in the overall objectives. By using this framework for all the service providers, the enterprise also benefits from a uniform method of reporting and, thereby, ready analysis and actions. This enhances the success of information security governance and the information security program even when the work is outsourced to distant locations.

Endnotes

1 Bakalov, Rudy; Feisal Nanji; “Offshore Application Development Done Right,” Information Systems Control Journal, vol. 5, 2005
3 ISACA, CISM Review Manual 2005, USA, 2005
4 Ibid.
6 IT Governance Institute, COBIT 4.0, USA, 2005, www.itgi.org

---

**Figure 6—Operational-level Scorecard: KGIs**

<table>
<thead>
<tr>
<th>No</th>
<th>Control/KGI</th>
<th>Target</th>
<th>Actual</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Number of violations of segregation of duties</td>
<td>0</td>
<td>0</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Number of users who do not comply with password standards</td>
<td>Max. 3</td>
<td>5</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Percentage of suspected and actual violations</td>
<td>Max. 5</td>
<td>2</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Percentage of critical assets covered by internal/external penetration tests</td>
<td>Min. 95</td>
<td>98</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Number of computers with patches behind agreed-upon SLA</td>
<td>Max. 2</td>
<td>1</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Number of outdated policies, procedures, standards and guidelines</td>
<td>Max. 4</td>
<td>5</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Number of internal audits scheduled</td>
<td>Min. 2</td>
<td>2</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Number of penetration tests not performed as required for the quarter</td>
<td>Max. 1</td>
<td>0</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Percentage of agents/employees trained on information security policies and procedures as part of induction</td>
<td>100</td>
<td>90</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Number of corrective/preventive actions taken based on analysis of logs</td>
<td>Min. 5</td>
<td>10</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Percentage of changes carried out as per change control procedure</td>
<td>100</td>
<td>90</td>
<td>Red</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Target and actual amounts are hypothetical figures for the purpose of this example. Categorization into green, amber and red is done on a predefined basis.
### Operation-level Performance Against KGI

<table>
<thead>
<tr>
<th>No</th>
<th>Control/KGI</th>
<th>Target</th>
<th>Actual</th>
<th>Status</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Number of obsolete accounts</td>
<td>Nil</td>
<td>5</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Number of unauthorized IP addresses and ports</td>
<td>Max. 5, 3</td>
<td>10, 5</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Number of cryptographic keys compromised and revoked</td>
<td>0</td>
<td>0</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Number of access rights revoked, reset or changed</td>
<td>Max. 5</td>
<td>3</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Number of security awareness training programs for agents/employees</td>
<td>Min. 10</td>
<td>11</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Percentage of agents/employees covered by fire/evacuation drill</td>
<td>Min. 95</td>
<td>95</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Percentage of agents/employees covered by BCP training</td>
<td>Min. 90</td>
<td>90</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Number of security awareness training programs for third-party employees</td>
<td>Min. 75</td>
<td>75</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Percentage of logs analyzed on a regular basis</td>
<td>Min. 90</td>
<td>95</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Number of dedicated security personnel at the offshore location</td>
<td>Min. 4</td>
<td>5</td>
<td>Green</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Target and actual amounts are hypothetical figures for the purpose of this example. Categorization into green, amber and red is done on a predefined basis.

---

**Sekar Sethuraman, CISA, CISM, CISSP, CIA, CSQA, BS7799 LA**

is currently head-IT security (Greater Asia) of LexisNexis.
He is also currently director-programs of the ISACA Chennai Chapter. He can be reached at sekar.sethuraman@lexisnexis.com.au.