## Contents

**Executive Summary**
- Overview ........................................ 3
- Key Findings .................................. 3
- Management Practices of Organizations with the Best Outcomes 3
- Management Practices of Organizations with Worse Outcomes 4
- Guidance and Recommendations .................. 5

**Benchmark Findings**
- Are Chief Information Security Officers Delivering Better Results? 6
- Will the Real CISO Please Stand Up .................. 7
- Larger Implications of Management Structure and Operational Strategy 8
- Establishing and Managing Objectives for Information Security and Assurance 9
- Managing Objectives and Specialization of Labor 10
- Managing Information Security and Assurance 11
- Standardizing Procedures and Improving Quality 12
- Managing Day-to-Day Operations .................. 14
- Automation of Standardized Procedures and Controls 16
- Measurement and Reporting ...................... 17
- Where Information Security Reports: Does it Matter? 17
- Rewards for Managing the Effort ................. 19

**About the Research** ............................. 20

**About IT Policy Compliance Group**
Executive Summary

Overview
This research report covers compiled findings from benchmarks conducted by the IT Policy Compliance Group on topics relevant to managing information security, including: organizational structure, operational strategies, management standards, and operations among others. The findings presented in this report are from benchmarks conducted from late 2008 through late 2009 and are organized by the outcomes organizations are experiencing.

Key Findings
Management practices of organizations with the best outcomes
The organizations with the best outcomes share several characteristics, including:

- Spending 50 percent less on audit each year
- The least data loss or theft and the lowest financial exposure from data loss
- The fewest hours of business downtime from IT failures or disruptions
- The highest rates of customer retention, revenue and profit

These organizations have a chief information security officer (CISO) or a senior manager of IT assurance who is in charge of information security. The CISO reports to either a chief risk officer (CRO), a chief compliance officer (CCO) or the senior manager of assurance.

IT is charged with defining and managing core standards for information integrity, availability and confidentiality.

The organizations manage business productivity and risks by using policies and targets for minimum acceptable downtime and maximum acceptable risks.

In addition, these organizations focus on operational excellence in IT by:

- Standardizing procedures and controls for information security.
- Widely adopting and implementing procedures from ISO, CobiT, ITIL, PCI and other frameworks.
- Managing information security through staff reporting to the CISO.
- Managing day-to-day operations through the CISO's staff and a staff of IT security operations specialists.
- Automating procedures and controls for information security.
- Measuring, assessing and reporting on risks daily, weekly and monthly.
- Implementing a quality assurance program.

1-in-10 organizations with the best outcomes

- Information security reports to a CRO, CRO or assurance manager
- Manager of information security is a CISO or senior manager of IT assurance
- IT drives and manages information integrity, availability and confidentiality standards
- Productivity and security are managed by policies and targets for minimum acceptable downtime and maximum acceptable risks
- Standardized procedures and controls are implemented
- Information security is managed by the CISO
- Day-to-day operations are managed by the CISO and IT security operations specialists
- Policies, procedures and controls are nearly fully automated
- Measurement and reporting occur daily, weekly and monthly
- A quality improvement program is implemented

Experience

Annualized data loss exposure: 0.4% of revenue
Business downtime: less than 4 hours
Regulatory audit spend: $1.30 relative to security
Revenue: 8.5% higher than industry average
Profit: 6.4% higher than industry average
Management practices of organizations with worse outcomes

In contrast, 7-in-10 organizations with normal industry outcomes and 2-in-10 organizations with the worst outcomes have very different organizational structures and operational strategies for managing information security. The differences include:

### 7-in-10 organizations with normal outcomes
- Information security reports to the CIO or the Vice President of IT operations
- Manager of information security is a CSO or a manager or director in IT operations
- Legal counsel defines and manages information integrity, availability and confidentiality standards
- Policies or targets for minimum acceptable downtime and maximum acceptable risks are not implemented
- A mixture of cherry-picked and ad-hoc procedures and controls are implemented
- Information security is managed by IT operations
- Day-to-day operations is managed by IT operations
- A mixture of manual and automated procedures and controls are employed
- Measurement and reporting occur quarterly to once every six-months
- A quality control program is not implemented

### Experience
- Annualized data loss exposure: 6.4% of revenue
- Business downtime: 4 to 59 hours
- Regulatory audit spend: $4.20 relative to security
- Revenue: even for industry average
- Profit: even for industry average

### 2-in-10 organizations with the worst outcomes
- Information security reports to the Vice President of IT operations, or the chief financial officer (CFO)
- Manager of information security is network or systems administrators
- Lines of business define and manage information integrity, availability and confidentiality standards
- Policies or targets for minimum acceptable downtime and maximum acceptable risks are not implemented
- Standardized procedures and controls are not implemented
- Information security is managed by IT operations
- Day-to-day operations is managed by IT operations
- Primarily manual procedures and controls are employed
- Measurement and reporting occur once every nine-months to once annually
- A quality control program is not implemented

### Experience
- Annualized data loss exposure: 9.6% of revenue
- Business downtime: 60 hours or more
- Regulatory audit spend: $1.50 relative to security
- Revenue: 8.5% less than industry average
- Profit: 6.9% less than industry average
Guidance and Recommendations

Wholesale organizational change is never recommended: it often introduces unintended consequences that take longer to reach parity. Nevertheless, the benchmark findings do suggest the following incremental changes:

- Change the reporting structure of the senior leader for information security to the CIO, CRO, CCO if the information security function currently reports into IT operations or the financial officer
- Appoint a CISO or a senior IT assurance manager for information security if one does not exist
- Establish an IT governance forum in the organization for two critical tasks:
  - Defining and managing information integrity, availability and confidentiality standards
  - Defining and managing minimum acceptable downtime and maximum acceptable risks
- If procedures and controls are not standardized, choose at least one standard and refine over time
- Manage information security through the senior leader of the function
- Consider establishing IT security operations specialists and an organization focused on day-to-day operations
- Migrate heavily manual procedures to standardized procedures that are automated by technology
- Establish a quality-improvement program for the information security and assurance program
- Aim for 75% automation of procedures and controls, but do this in demonstrable increments
- Increase the rate of measurements to monthly, then weekly and finally daily
- Report using key metrics, indicators, results, and implications

Organization of the Report
There are three sections to this report, as follows:

**Executive Summary:** contains the key findings of the research and recommendations for best practices for managing information security.

**Benchmark Findings:** covers in detail the principal management and organizational practice findings as these relate to outcomes.

**Research Background:** covers the sample and demographics of the benchmarks conducted.
Benchmark Findings

Are Chief Information Security Officers delivering better results?

Benchmarks conducted during the past year show that one of the dominant factors influencing outcomes being experienced by organizations related to the loss or theft of customer data, is whether a Chief Information Security Officer (CISO) is in charge of the information security and assurance function of the organization.

Only 1-in-10 organizations are experiencing the best outcomes with the lowest rates of customer data loss and theft with less than 3 events annually. About 7-in-10 organizations are experiencing normal outcomes with elevated numbers of data loss and theft events, ranging from 3 to 15 of these each year. Nearly 2-in-10 organizations are experiencing the worst outcomes with the highest rates of data loss and theft each year with more than 16 such events.

Among the organizations with the least amount of data loss and theft, almost 8-in-10 report having a CISO who manages the information security and assurance function while only 2-in-10 organizations do not. Of the organization with higher but normal levels of data loss and theft, 6-in-10 report having a CISO who manages the information security and assurance function, while 4-in-10 organizations do not. Among the organizations with the worst and highest levels of data loss and theft, 4-in-10 organizations report having a CISO in charge of the information security and assurance function while 6-in-10 do not (Figure 1).

Figure 1: Organizations with CISOs deliver better results

Key insights into organizational and operational strategies reveal the success factors being used by organizations with the best outcomes that include:
- Significantly reduced costs
- Much lower financial risk and loss
- Better business results

Although the odds appear to indicate that CISOs deliver better outcomes, nearly 40 percent of the organizations experiencing the most customer data loss and theft also claim to have a CISO managing the information security function. As a result, this cannot be the only factor at work in delivering better results. Key insights into organizational and
operational strategies from ongoing benchmarks reveal the success factors being used by organizations with the best outcomes: significantly reduced costs, much lower financial risk and loss, and better business results.

**Will the real CISO please stand up!**

Not all organizations claiming to have a CISO actually employ someone with the “CISO” title. Despite this, a majority (about half or 45 percent) of the organizations with the best outcomes actually have a named CISO managing the information security and assurance function.

Compared to all other organizations, those with a named CISO are 10 times more likely to experience the least loss of theft of customer data. After a named CISO, those that manage the information security function through a senior manager of IT assurance are four-times more likely to experience less loss or theft of customer data than all other organizations.

In contrast, organizations where the information security function is being managed at lower levels within IT operations by systems and network administrators or by managers in IT operations are 4-to-8 times more likely to be among those with the highest rates of data loss and theft.

Between these two extremes are organizations that are managing the information security through either the vice president of IT operations or a named chief security officer (Figure 2).

**Figure 2: Title of the person in charge of information security**

![Title of the person in charge of information security](image)

There are two important findings about management structure related to the information security function, as follows: 1) Worse outcomes are occurring among organizations managing the information security function at lower-levels within IT operations; and 2) Better outcomes are occurring among organizations managing the information security function outside of IT operations by a CISO or a senior IT information quality assurance manager.

A common management approach to information security — that security is only a technology issue — may be at the root of the problem for organizations experiencing the highest rates of data loss and theft. These organizations manage the function deep within the bowels of IT operations with less management oversight and control. As the benchmark findings show, organizations with the most success are managing information security at a higher level as a quality-controlled function that includes and goes beyond the technologies involved.
Larger implications of management structure and operational strategy

Beyond a better track record for protecting customer data, organizations with CISOs or senior managers of IT assurance who manage the information security function also post much better results across other measures.

The same 1-in-10 organizations with the best track records for protecting customer data, where a CISO or IT assurance manager are in charge of managing information security, also experience better outcomes across other dimensions tracked by the benchmarks, including:

- Much lower spending on regulatory audit
- Less business downtime due to failures or disruptions in IT
- Much higher customer retention rates, revenue and profit

As the benchmark findings reveal, management structure for the information security function is directly related to lower costs, reduced risks, and much better top-line results (Figure 3).

**Figure 3: Outcomes from worst to best**

```
Normal outcomes
7 in 10
2,350 of 3,408 (69%)

Worst outcomes
2 in 10
645 of 3,408 (19%)
```

<table>
<thead>
<tr>
<th>Costs</th>
<th>Best outcomes</th>
<th>Normal outcomes</th>
<th>Worst outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spend on audit (per $ spent on information security)</td>
<td>$1.50</td>
<td>$3.50</td>
<td>$4.20</td>
</tr>
<tr>
<td>Downtime from IT failure and disruptions</td>
<td>10% of revenue</td>
<td>3% of revenue</td>
<td>1% of revenue</td>
</tr>
<tr>
<td>Exposure to loss of customer data</td>
<td>9.6% of revenue</td>
<td>6% of revenue</td>
<td>6.4% of revenue</td>
</tr>
<tr>
<td>Results</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer retention</td>
<td>-3.6%</td>
<td>-3.2%</td>
<td>-0%</td>
</tr>
<tr>
<td>Revenue</td>
<td>-5.5%</td>
<td>-4.3%</td>
<td>-0%</td>
</tr>
<tr>
<td>Profit</td>
<td>-6.9%</td>
<td>-3.5%</td>
<td>-0%</td>
</tr>
</tbody>
</table>

By comparison, the 7-in-10 organizations operating at the norm include most organizations managing the information security function through a chief security officer or the senior manager of IT operations. These organizations are spending three times more on regulatory audit than all others, are exposed to higher financial risks from the loss of customer data, higher financial risks due to business outages from IT failures, and are posting lower results for customer retention, revenue and profit.

In contrast, the 2-in-10 organizations with the worst outcomes are dominated by organizations managing the information security function from lower-levels within IT operations. Although these organizations are spending only marginally more on regulatory audit, they are experiencing the highest levels of business disruption due to failures and disruptions in IT, the most customer data loss and theft, and the worst track-records for customer retention rates, revenue and profit when compared with other organizations. The results are undeniable: better managed organizations are spending less on regulatory audit, are exposed to much less financial risk and are posting superior business results.

Source: IT Policy Compliance Group, 2010
Establishing and managing objectives for information security and assurance

The benchmarks also reveal significant organizational differences, by whom and which functions, are primarily responsible for defining organizational standards for information integrity, availability and confidentiality.

For example, the 2-in-10 organizations experiencing the worst outcomes predominantly establish core information assurance and security standards through lines of business. The business divisions defining organizational standards for information availability, integrity and confidentiality in these organizations are accompanied by fewer where legal counsel, IT and human resources define the primary information security and assurance objectives for the organization.

Among the majority — 7-in-10 — with normal outcomes, legal counsel is in charge of defining information integrity, availability and confidentiality standards, accompanied by IT.

The profile among the 1-in-10 best performing organizations is starkly different: more than half of these organizations rely on IT to define the core standards for information integrity, availability and confidentiality. These are accompanied by fewer where legal counsel is in charge, and fewer where business lines and human resources are in charge of establishing these objectives (Figure 4).

Figure 4: Organization and information assurance objectives

Placing business lines in charge of defining objectives for information integrity, availability, and confidentiality is a little like putting the fox in charge of the proverbial hen-house: moreover, the worst business results, highest financial risks and operational costs are proof this approach does not work.

Charging legal counsel to define these objectives may deliver protection from litigation, but it is coming at the expense of less than optimal business results, higher operating expenses and higher financial risk from the loss or theft of data.

Although IT better understands information integrity, availability and confidentiality, success depends on a collaboration between multiple parties, including business line managers, legal counsel, business divisions, human resources, and the audit and risk committee. Managing IT governance objectives, including information integrity, availability and confidentiality; should be a collaborative effort.

The challenge for many organizations will be to right-size organizational collaboration to establish and manage critical goals and objectives for securing and managing information assets. While IT may be better positioned to interpret operational and assurance objectives, it will be most successful where the organization is involved.
Managing objectives and specialization of labor

In addition to management structure and strategy for the information security and assurance function, two of the defining differences related to outcomes being experienced by organizations are: 1) Balancing business productivity related to the use of IT, and 2) The specialization of labor within IT to achieve the balance.

Among the organizations where the information security function is managed by a CISO or a senior manager of IT assurance, the use of policies describing minimum service levels and maximum acceptable risks are almost always implemented.

This is in sharp contrast with organizations where the information security function is being managed by systems administrators or IT operations managers, where such policies and objectives for minimum IT service levels and maximum acceptable risks are either never implemented or are rarely implemented (Figure 5).

Figure 5: Most common and least common policies

<table>
<thead>
<tr>
<th>Policies implemented</th>
<th>Policies never implemented</th>
</tr>
</thead>
</table>
| - Acceptable usage by employees
- Security for networks, systems, databases and applications
- Procedures in IT | Policies are never implemented |
| Managements' policies with the widest range of implementation |
- Minimum acceptable service levels
- Maximum acceptable risks
- Monitoring and reporting
- Changes to policy |

Worst results
Normal results
Best results

Source: IT Policy Compliance Group, 2010

The best performing organizations clearly define minimum service levels and maximum acceptable risks, while dividing responsibilities between IT operations and the information security and assurance functions.

Among these organizations, IT operations personnel are focused almost exclusively on delivering the highest levels of service while information security personnel are focused exclusively on delivering the highest levels of information assurance. Defined policies and targets for minimum acceptable service levels and maximum acceptable risks are used to define the boundaries for managing worst-case exceptions. When service levels degrade to unacceptable levels, proscribed management and operational actions are undertaken. Similarly, management and operational actions are engaged when unacceptable risks are occurring.

In contrast, organizations with the worst results do not define management objectives in the form of policies and targets for minimum acceptable service levels or maximum acceptable risks. Without guidelines, business productivity levels and information assurance results are worse. As the benchmarks reveal, operating without management policies and targets for minimum acceptable downtime and maximum acceptable risk is not working.

Moreover, organizations that do not divide the responsibilities for managing operational availability from managing information security assurance are the same organizations with the worst outcomes.
Managing information security and assurance

In an attempt to delineate the impact that organizational structures are having on outcomes being experienced by organizations, three different groups of IT staff responsibilities were benchmarked. The organizations within IT that were tested include: staff reporting to IT operations; staff reporting to the CISO or senior manager of information assurance; and a staff of IT security operations specialists that may have different reporting relationships. Groups of management and operational activities were benchmarked against outcomes: one focused on information security management activities and another on day-to-day execution of information security and assurance activities.

Examples of management activities tested include maintaining security standards and frameworks, conducting risk assessments, reporting on business risks related to the use of IT, and establishing and managing budgets for the information security function. In general, the findings show a majority of the best performing organizations implement management activities with specialist IT security operations staff, or staff reporting to the CISO.

For some of the management activities, distinct differences exist among the best performing organizations. For example, best performing organizations tend to have staff reporting to the CISO manage the budgets, report on business risks, while also being responsible for establishing and maintaining information security policies. Other findings indicate a specialist IT security operations staff is more commonly being tasked to maintain evidence about compliance with regulatory mandates, and in some cases is equally capable of conducting risk assessments and establishing information security standards and frameworks (Figure 6).

**Figure 6: Management activities among best performing organizations**

![Graph showing management activities among best performing organizations](image)

Although variations in reporting relationships exist from one organization to the next, what is clear from the findings is that better outcomes are more difficult to find among the organizations where staff reporting to IT operations is charged with the activities to manage information security and assurance.

These findings are in keeping with the overarching evidence that worse outcomes are the norm among organizations where information security and assurance is being managed from within IT operations.

Whether or not a specialist IT operations staff exists, the findings reinforce the discontinuity between outcomes and the organizational structure for the information security and assurance function. Among organizations with an IT security operations staff, the dominant recruiting-ground often comes from IT operations. As one senior manager recently
stated, “we always recruit (for IT security operations) from (IT) operations. These people understand our business, are already familiar with our technology, and just have to be groomed and mentored to make the transition (to IT security operations).

Despite the recruitment of staff from IT operations, the findings show there are very real differences in outcomes, based on which staff is tasked with managing the objectives established for the information security and assurance function.

When many of the activities tested against outcomes are presented, a rather stark picture emerges of the organizational impact on outcomes. The findings show a clear distinction in outcomes — by different management activities — between staff reporting to IT operations, or staff reporting to a CISO or the senior information security assurance manager (Figure 7).

**Figure 7: Managing information security**

Organizational function with primary management responsibilities

- Staff reporting to IT operations
- Staff reporting to IT security operations manager
- Staff reporting to senior information security manager

| Establishes/maintains information security policies | 2 in 10 with worst outcomes |
| Establishes/maintains security standards and frameworks | 7 in 10 normative outcomes |
| Delivers user training and awareness | 1 in 10 with best outcomes |
| Conducts risk assessments |
| Assesses/reports on procedural controls |
| Assesses/reports on technical controls |
| Maintains control objectives |
| Reports on business risks related to the use of IT |
| Reports on policy compliance in IT |
| Reports on regulatory and legal compliance in IT |
| Established/manages information security budgets |
| Maintains evidence of compliance |

*Source: IT Policy Compliance Group, 2010*

Although the picture presents a rather sharp-edged view of the relationship between outcomes and who is performing these management activities, there are subtler differences by individual organization. For example, one firm with best outcomes actually employs outsourced contractors as its IT security specialists to manage outsourced IT operations, all of which are managed by an internal CISO and internal staff reporting to the CISO.

Another organization splits the IT security operations specialist function geographically but maintains central control through a staff reporting to the CISO. A different organization employs a small staff reporting to the CISO and places most of its emphasis on a much larger and more experienced IT security operations staff, some of which is being delivered through contractors.

Differences in organizational structure are to be expected, even among the best performing organizations. For this reason wholesale organizational change is not recommended. However, one of the clear findings from the benchmarks is that managing information security and assurance from within IT operations is no longer done by organizations with the best outcomes.

**Standardizing procedures and improving quality**

Standardized practices and procedures, first pioneered by Henry Ford, made it possible to achieve much higher output at lower costs. However, lower cost and higher output do not yield high-enough quality. And if there is anything the information security and assurance function is about, it is quality.
The focus on quality may not be apparent on the surface for many senior managers outside IT because the only thing they, and the rest of the organization may know about its information security and assurance function is when something goes wrong. When a malware attack places the organization’s information assets at risk, or when a virus shuts down production systems on a factory floor, or when the theft of customer data makes the headlines of the business press, then the organization knows about its information security and assurance function. Unfortunately a steady drumbeat of negative news-events, sometimes over-hyped, hides the 99.9 percent of instances when the information security and assurance function succeeds by detecting and preventing high risks from snowballing out of control.

Nevertheless, quality control is what the information security and assurance function is about, and its efforts are focused on one of the most important assets of the firm: its information assets and the information assets entrusted to it by its customers, partners and suppliers.

Achieving lower cost objectives through the use of standardized procedures and achieving higher levels of quality, first introduced by Edward Deming in Japan, has evolved into Six Sigma and similar quality improvement programs throughout the industrialized World. Ongoing discussions with CISOs responsible for information security and assurance verify that “Six-Sigma-like” quality assurance programs are becoming more common to improve results for information security and assurance efforts. However, many of these CISOs also advise that quality-levels cannot be consistently improved without the uses of standardized procedures.

Standardization among organizations with best performance outcomes is reflected in the widespread adoption and implementation of standardized frameworks for policies, procedures and practices for information security and assurance. Some of these standardized practice and policy frameworks include ISO, CobiT, COSO, NIST, CIs, PCI, and HIPAA defined practices and policies among others. Recent tests show that the use of standardized policy and procedures guidelines is dominant among organizations with the best outcomes, whereas their use is dormant among those with the worst outcomes (Figure 8).

**Figure 8: Framework guidelines and standardized procedures**

![Figure 8](image)

Source: IT Policy Compliance Group, 2010

A few examples may provide additional insight into how these guidelines are being used. The IT governance committee at a large utility decided four years ago to standardize on the use of CobiT to guide its IT assurance, audit and information security practices. Electing to employ CobiT as its standard to drive improvement, the CISO said “We had to choose one (framework) to make progress, so we picked CobiT. Otherwise we’d still be operating (information security) without...
guidelines." Today the organization has streamlined its information security and assurance activities, while developing greater confidence that an upcoming regulatory audit of its practices will be much easier to demonstrate.

A well-known organization selected the Information Technology Infrastructure Library (ITIL) to define service-level agreements to measure itself, as well as its suppliers and contractors. Due to weaker-than-desired coverage in ITIL for information security and assurance, the organization added ISO 27001 defined-practices. The CISO of this organization recently said, "After we defined the procedures and practices, it was simple to see where the overlaps were and what wasn't getting done."

Another brand-name organization implemented ISO-based procedures complemented with CIS checks for its technical controls. The external auditors mapped their CobiT controls to both the firms ISO practice-controls and CIS technical controls, which dramatically reduced expenses from unplanned rounds of controls testing that were required prior to the adoption of these standardized procedures and control-checks. Whatever is selected and employed to standardize procedures and improve quality-levels, it is important to ensure that these map to actual activities being measured for improvement, including day-to-day operations for information security and assurance.

Managing day-to-day operations

Much like the management activities tested by the benchmarks, day-to-day tasks in delivering information security and assurance were benchmarked to distill differences in outcomes by organizational strategy with groups of operational activities tested against three different staffs: IT operations staff, IT security operations specialists, and staff reporting to a CISO.

We expected IT operations staff would demonstrate better outcomes for day-to-day operations. Some of the activities tested include: scanning networks, systems and applications; operating systems, networks, devices and applications; applying and testing patches for IT systems, networks and applications; maintaining security for gateway systems such as Email and Web systems; and maintaining access controls for people and IT assets.

However, the best outcomes for information security and assurance are being delivered by the organizations where day-to-day operational activities are being delivered by either an IT security operations staff, the staff reporting to the CISO, or both. Results from the benchmarks demonstrate very low implementation of day-to-day activities by IT operations among the organizations with the best outcomes, although a few of the activities showed higher-levels than the management tasks (Figure 9).

Figure 9: Day to day tasks among best performing organizations

1: Scans networks, systems and applications
2: Operates IT configuration tests on IT infrastructure
3: Operates IT security tests
4: Operates regulatory audit tests

Source: IT Policy Compliance Group, 2010
Best Practices for Managing Information Security

Among organizations with the best outcomes, an IT security operations staff is better positioned to deliver better results for activities that include scanning networks, systems and applications, and operating detailed tests involving configurations and settings on systems, networks, databases and applications. In addition, some day-to-day tasks are better performed by staff reporting to the CISO, most notably operating overall security tests and regulatory audit tests.

Although there are some variations, what is clear from the findings is that better outcomes are more difficult to find among organizations where staff reporting to IT operations is delivering day-to-day information security and assurance activities.

Much like the management activities tested, a rather stark picture emerges of the relationship between outcomes and day-to-day activities for the information security and assurance function. The best outcomes, contrary to original supposition, are actually being delivered by organizations that implement day-to-day activities by a combination of an IT security operations staff and staff reporting to the CISO (Figure 10).

**Evolution of information security and assurance at an insurance company**

This organization did not have a specialized IT security operations team and instead managed day-to-day activities delivered by IT operations with a dotted-line management structure to a very small staff reporting to the CSO. Information security was funded and operated within lines of business, with uneven results and high exposure to system IT threats resulting in unacceptable data loss and theft events. After three years with no substantial improvements against internal metrics and external audits, the organization implemented a beefed-up swat-team that evolved into a full-time IT security operations staff.

Today the IT security operations team reports to a CISO who reports to the CIO and the chief risk officer, and the company has reduced its data losses. While not among the best performers, the organization is now within striking distance and the most recent audit covering IT controls reveals substantial improvement due to its standardized procedures, division of labor, automation, measurement, reporting and quality program.

**Figure 10: Managing Day-to-Day Operations**

Organizational function with primary operational responsibilities

- Staff reporting to IT operations
- Staff reporting to IT security manager
- Staff reporting to senior information security manager

<table>
<thead>
<tr>
<th>Scans networks, systems and applications</th>
<th>2 in 10 with worst outcomes</th>
<th>7 in 10 normative outcomes</th>
<th>1 in 10 with best outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conducts intrusion detection and vulnerability analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operates IT configuration tests on IT infrastructure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operates IT security tests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operates regulatory audit tests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operates tests of controls and patches</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applies patches to networks, systems, applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintains security controls, configurations and patches</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintains user access controls and authorizations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintains security for Email and Web systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivers and manages IT security incident response</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Source: IT Policy Compliance Group, 2010*

Although the picture that emerges presents a rather sharp-edged view of the relationship between outcomes and who is performing day-to-day activities, there are subtler differences by individual organization. For example, a Bank uses its IT operations center to manage information security and assurance with co-located IT security operations personnel who report to the CISO. This organizational model works for the Bank: it is among the 1-in-10 organizations reporting superior performance results on all metrics tested by the benchmarks.
Despite this example and other management reporting structures, organizations with worse outcomes are among those where the IT operations staff is responsible for delivering day-to-day information assurance and security.

**Automation of standardized procedures and controls**

The automation of standardized policies, practices and controls plays an important role for organizations experiencing the best outcomes. Among these organizations, an average of two-thirds (66 percent) of procedures and controls related to the information security and assurance function are fully automated. In comparison, about half (49 percent) of the controls for information security and assurance are automated by organizations experiencing normal outcomes.

Among organizations with the worst outcomes, the level of automation is the lowest, with less than one-third (33 percent) of procedures and technical controls being fully automated (Figure 11).

**Figure 11: Automation and controls**

<table>
<thead>
<tr>
<th>Outcomes</th>
<th>Automated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worse</td>
<td>30%</td>
</tr>
<tr>
<td>Normal</td>
<td>49%</td>
</tr>
<tr>
<td>Best</td>
<td>75%</td>
</tr>
</tbody>
</table>

In addition to a higher automation profile among best performing organization there is an even mix of procedural and technical controls to manage business risks related to the use of IT. This is in sharp contrast to the worst performing organizations where procedural controls for managing risk related to the use of IT are dominant. Reflecting higher use of more error-prone, and more costly manual procedures, organizations experiencing worse outcomes are unable to leverage the benefit of automation due to non-standardized procedures.

Standardization and automation go hand-in-hand, as Ford, Deming and many companies have proved. Low standardization of procedures is synonymous with an inability to automate, whereas more standardized procedures and controls means that more can be automated. A quality control effort for standardized procedures appears to be one of the engines for better information security and assurance results that include: lower costs, higher quality, reduced risk and better business results.

Best performing organizations consistently automate procedures and controls, including: ongoing assessments of systems, networks, databases and applications; penetration testing; vulnerability and remediation management; entitlement and access controls; data leakage controls; the management of IT asset endpoints; procedures for handling information and IT assets; policy violation reporting; mappings between policies, controls, regulatory and legal mandates; management reporting and scorecards among others.

Better outcomes are the direct result of standardizing and automating procedures, measuring results and making improvements.
Best Practices for Managing Information Security

Measurement and reporting
Measurement and reporting are hallmark procedures that are nearly fully automated by organizations with the best outcomes. As a central tenet of the information assurance and security program, the best performing organizations automate measurements of key risks, indicators, and report on these very frequently.

Among the types of measurements and reports automated by best performing organizations are those involving: user accounts, entitlements, privileged accounts, and privilege-escalations; the assessment of IT asset, configurations and settings; and the effectiveness of controls for managing risks related to the use of IT (Figure 12).

Figure 12: Assessment and reporting rates

<table>
<thead>
<tr>
<th>Operational controls and measurement</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency of management (days)</td>
<td>Worst</td>
</tr>
<tr>
<td>user accounts</td>
<td>207</td>
</tr>
<tr>
<td>IT assets</td>
<td>239</td>
</tr>
<tr>
<td>IT controls</td>
<td>222</td>
</tr>
</tbody>
</table>

Simply put: best performing organizations assess and report on key risks, controls and indicators on a daily, weekly and monthly basis. In contrast, normative performing organizations assess and report between once per quarter to once every five-to-six months. The worst performing organizations assess and report in time-frames that are beyond five months. For some of the worst performing organizations, an annual audit involving IT is apparently too frequent.

As the quality assurance discipline found, measurement, reporting and comparison are keys to improving results, reducing costs and eliminating defects. The benchmarks show the same is true for the information assurance and security function.

Where information security reports: does it matter?
Does it matter where information security and assurance functions report in the organization? Some of the recent benchmarks attempt to answer this question, with varied results. But the relevant questions may not be to whom or where the functions report, but where the functions should not report.

Organizations experiencing better outcomes have the information security and assurance function reporting to one of three managers. These include:
- A chief risk officer (CRO)
- A chief compliance officer (CCO)
- A Vice President or senior manager of IT assurance
In contrast to the best performing organizations, the 7-in-10 experiencing normal outcomes place the information security and assurance function reporting to the CIO or the senior manager of IT operations. Lastly, organizations with worst outcomes have the information security and assurance function reporting to the CFO or a senior manager in charge of IT operations (Figure 13).

**Figure 13: Where the information security function reports**

With the exception of the two opposite ends of the performance-spectrum (finance and IT operations on the worst end; risk, compliance and IT assurance on the best end), the results of the early benchmark tests are not conclusive enough to warrant overhauling existing reporting relationships where the function reports to the CIO.

For example, organizations with alternate reporting relationships and best performance-profiles include a company in the entertainment business with a CISO reporting directly to the CIO and dotted-line to the CEO. Another best-performing organization in the financial sector has a CISO reporting directly to the CIO and dotted-line to the audit committee of the board of directors. Another best-performing organization in the manufacturing sector has a CISO reporting to the CIO and dotted-line to the COO.

Although these are but some of the alternate reporting relationships for the information security and assurance function among best-performing organizations, the key points are these organizations implement other organizational strategies common to the best performers, including:

- CISOs managing IT security and assurance reporting to senior managers
- The adoption and use of standardized procedures and controls
- Very high levels of automation for standardized procedures
- Very frequent measurement and reporting
- A focus on managing quality for key risk and performance metrics

Senior-level reporting arrangements other than IT operations and finance are producing better outcomes where the organizational and operational strategies uncovered by these benchmarks are being implemented.
While “make sure we don’t get into the paper (for a data loss)” is the normal yardstick by which senior managers evaluate the effectiveness of information security and assurance, the improvements to top-line results (better customer retention, higher revenue and profit) are being posted by the best performing organizations.

**Rewards for managing the effort**
Aside from reputational and financial risk from the loss or theft of customer data, is it worth spending money to improve the information security and assurance function? The most value will be realized by the 2-in-10 operating with the worst outcomes. However most organizations are operating with normal results and will be able to improve results sooner. The benefits of improving the information security and assurance function fall into three categories: reducing the expense of audit, reducing risks associated with the use of IT, and improving top-line results.

**Reducing costs**
The average amount spent on audit by organizations with normal outcomes is $3.70 for every dollar spent on the information security and assurance function. In contrast, the amount spent on audit by the best performing organizations is $1.30 for each dollar spent on information security and assurance. The difference — $2.40 in audit expense reductions for each dollar spent on information security — is a very attractive return. Of course, this will be reduced as marginal returns occur with increasing effectiveness. Nevertheless, for most of the 7-in-10 organizations, these returns are worth the effort.

The research reveals savings on expenses for audit are coming from two contribution areas: 1) reductions in spend within IT to support audit due to the automation of heavily manual and error-prone procedures, and 2) reductions in spend on external audit services. Of the two, the returns for automating manual procedures are being reported as reaching break-even in short time-frames, typically a year or less. However, the reductions in external expenses for audit are cited as taking place over longer two-and-three year periods as audit cycles and contracts are adjusted.

**Reducing risks**
Based on the likelihood of data loss or theft and downtime from IT failures, the annualized value at risk for most organizations is 0.7 percent of revenue for business downtime, and 3 percent of revenue for the loss or theft of customer data. In comparison, the annualized value at risk for best performing organizations is 0.1 percent of revenue for downtime and 0.2 percent of revenue for customer data loss or theft. The difference — avoiding expenses amounting to 0.6 percent of revenue from downtime and 2.8 percent of revenue from data theft and loss — is worth the effort to improve results.

For many, the loss or theft of data resulting in financial damage seems remote or unlikely: “Data loss won’t happen to us”, is the operative posture. However, the senior managers of nearly 2,000 organizations that experienced data breaches and losses since 2005, many resulting in public exposure and unanticipated costs for litigation, cleanup, investigation and customer notification also believed it would never happen to them. The financial loss ratios are in-line with financial reports and the benchmarks conducted with more than 3,000 organizations.

Just ask the CEO of a major firm who awoke one morning to find her organization’s customer data and credit cards had been stolen and resold for pennies on the dollar. Not just any breach, but one that cost this organization more than $550 million in unanticipated expenses and more than a 10 percent decline in shareholder value. Totaling more than 8 percent of annual revenue, the managers of this organization never believed it could happen to them either. Today, “we manage and operate it (the information security and assurance function) very differently than before (the data theft event).”

**Improving results**
The information security and assurance function is not normally measured by better top-line results by most organizations. However, among the best performing organizations with CISOs managing the information security and assurance function, better top-line results are in the job description.

As one CISO said, “Part of my job is to leverage the technology to boost profits and reduce costs. I’m always showing (the business-lines) how we can (safely) use technology to make more (money).”

“I’m always showing the business lines how we can (safely) use technology to make more (money)."

- CISO of a F1000 organization
Best Practices for Managing Information Security

About the Research

Topics researched by the IT Policy Compliance Group (IT PCG) are part of an ongoing calendar established in consultation with advisory members, general members, and supporters of the Group, as well as from findings compiled from ongoing research. In addition to specific tracking questions common to each benchmark, the research is designed to uncover the relationship between business results, the actions organizations take in response to business pressures, the practices implemented, and the capabilities organizations use to respond to business pressures.

This report covers research findings for practices implemented for managing the information security and assurance function and are organized by outcomes being experienced. Benchmarks, including findings on outcomes, organizational structure, organizational strategy, and organizational dynamics for the information security function are covered by this report. The organizational study benchmarks were completed in December 2008 with respondents from 254 organizations, March of 2009 with respondents from another 354 organizations, and October 2009 with respondents from 201 organizations. In addition aggregated findings on outcomes covering more than 3,000 organizations are included in this report.

All of the organizations (100 percent) participating in the organizational structure and strategy benchmarks are located in North America and the findings have different errors, with the low being +/- 5 percent and the high being +/- 7 percent. The inherent error of the aggregated outcome findings is +/- 3 percent. Findings based on aggregated findings are accomplished after a normal distribution is identified using the same questions and answers options. The normative bands on outcomes have not changed over the aggregated benchmarks, indicating consistency across the many different organizations participating.

Industries represented

Almost every industry has participated in the benchmarks, including accounting services, advertising, aerospace, agriculture, apparel, architecture, automotive, banking, chemicals, computer equipment and peripherals, computer software and services, construction, consumer durable goods, consumer electronics, consumer packaged goods, distribution, education, engineering services, financial services, general business and repair services, government (local, state and federal level public administration), government (defense and intelligence), health, medical and dental services, insurance, law enforcement, legal services, management services, scientific and consulting services, manufacturing, medical devices, metals and metal products, mining, oil and gas, paper, timber and lumber, pharmaceuticals, public relations, publishing, media and entertainment, real estate, rental and leasing services, retail trade, telecommunications equipment, telecommunication services, transportation and warehousing, travel, accommodation and hospitality services, utilities, waste management and wholesale trade. The largest industries represented by the benchmark findings include healthcare, financial services and manufacturing, each of which account for seven percent of participating organizations. Education and government (public administration at local, state and federal levels) each represent five percent of the sample. All other industries account for less than five percent of benchmark participants.

Revenue of participating organizations

Thirty percent of the organizations participating in the organizational study benchmark have annual revenues or budgets that are less than $50 million. Another 28 percent have annual revenues or budgets that are between $50 million and $999 million. The remaining 42 percent have annual revenues or budgets that are $1 billion or more.

Functional areas of responsibility

Sixty-nine percent of the participants in the organizational study benchmarks work in IT, 15 percent of these participants work in finance and internal controls, and 9 percent work in legal and compliance functions within their organizations. The remaining seven percent of qualifying participants work in a wide range of job functions, including senior managers responsible for customer service, sales, marketing, manufacturing and development functions.

Job titles of participants

Thirty-six percent of the participants in the organizational study benchmarks are senior managers, 15 percent are vice presidents, 32 percent are managers or directors, and 17 percent are staff.
About IT Policy Compliance Group
The IT Policy Compliance Group is dedicated to promoting the development of actionable findings that will help organizations meet their IT policy and regulatory compliance objectives. The Group Web site at www.itpolicycompliance.com features content by some of the leading experts in the world of IT and regulatory compliance, interactive self assessment tools, published research reports, resource links and educational seminars being conducted around the World.

The Group’s research is designed to help IT, legal, financial, and internal control professionals to:

- Benchmark results and efforts against peers and best-in-class performers
- Identify key drivers, challenges, and responses to improve results
- Determine the applicability and use of specific capabilities to improve results
- Identify best practices based on results of the benchmarks

The Group relies upon its advisory members, associate members, supporting members and significant benchmark findings to drive its research and editorial calendar.

IT Policy Compliance Group Charter Members

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
+1 (650) 527 8000
www.symantec.com
info@symantec.com

The Institute of Internal Auditors
247 Maitland Avenue
Altamonte Springs, FL 32701
+1 (407) 937 1100
www.theiia.org
iaa@theiia.org

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008
+1 (847) 253 1545
www.isaca.org
info@isaca.org

Computer Security Institute
600 Harrison Street
San Francisco, CA 94107
+1 (415) 947 6320
www.gocsi.com
csi@cmp.com

Protiviti
New York Office
1290 Avenue of the Americas, 5th Floor
New York, New York 10104
+1 (212) 603 8300
www.protiviti.com
info@protiviti.com

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008
+1 (847) 660 5600
www.itgi.org
info@itgi.org

IT Policy Compliance Group Advisors
A current list of advisors can be found on the IT Policy Compliance Group website.
Founded in 2005, the IT Policy Compliance Group conducts benchmark research focused on delivering fact-based guidance on the steps that can be taken to improve results. Benchmark results are reported through www.itpolicycompliance.com for the benefit of members.

IT Policy Compliance Group

Contacts:
Managing Director: Jim Hurley
Telephone: +1 (216) 373 7010
jhurley@itpolicycompliance.com
Managing Editor: John Ortbal
Telephone: +1 (847) 444 0344
jortbal@itpolicycompliance.com
www.itpolicycompliance.com

February 2010

The information contained in this publication has been obtained from sources that the IT Policy Compliance Group believes to be reliable, but is not guaranteed. Research publications reflect current conditions that are subject to change without notice.

Copyright © 2010 IT Policy Compliance Group. Names and logos may be trademarks of their respective owners.
All rights reserved. 2/10