The internal audit and information security functions should play complementary roles in an organization’s information security program. The information security function should focus on the design and implementation of the security plan, while internal audit should assess and evaluate the functioning of the plan’s components. Yet, in practice, the relationship between the two functions is not always positive.

At its worst, the relationship can become so adversarial that it impairs effective governance, as exemplified by one information systems (IS) manager: “…It has been a game of cat and mouse. The auditors are trying to catch IT doing something and IT is trying to prevent audit from finding out.” In part, this may reflect the general friction between the accounting and IS functions. But, it also likely reflects the tension that exists among the information security function and other compliance-oriented groups (e.g., records management) within the organization.

What causes friction between the internal audit and information security functions? What actions can management take to improve that relationship? What are the benefits, if any, of having a better relationship between internal audit and information security?

A multistage research program was undertaken to answer these questions. First, in-depth interviews with both internal audit and information security professionals at four organizations were conducted. Then, the insights from those interviews were used to design two survey-based studies. The first survey collected data from IS professionals across a variety of industries, the results of which are analyzed here, and the other collected data from internal auditors, the results of which will be analyzed in part 2. Figure 1 shows the characteristics of the information security professionals who completed the survey.

**Figure 1—Characteristics of Survey Participants**

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Mean</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work experience (years):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With current employer</td>
<td>6.8</td>
<td>1-27</td>
</tr>
<tr>
<td>• Total</td>
<td>23.1</td>
<td>1-42</td>
</tr>
<tr>
<td>Organization has a chief information security officer (CISO).</td>
<td>17</td>
<td>68%</td>
</tr>
<tr>
<td>Information security reports to the chief information officer (CIO).</td>
<td>17</td>
<td>68%</td>
</tr>
<tr>
<td>Internal audit is in-house.</td>
<td>18</td>
<td>72%</td>
</tr>
<tr>
<td>Respondent certified as a Certified Information Systems Security Professional (CISSP)</td>
<td>18</td>
<td>72%</td>
</tr>
<tr>
<td>Industry:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Government</td>
<td>6</td>
<td>24%</td>
</tr>
<tr>
<td>• Manufacturing</td>
<td>5</td>
<td>20%</td>
</tr>
<tr>
<td>• Financial services</td>
<td>5</td>
<td>20%</td>
</tr>
<tr>
<td>• Technology</td>
<td>3</td>
<td>12%</td>
</tr>
<tr>
<td>• Health care, education and other professional services</td>
<td>6</td>
<td>24%</td>
</tr>
</tbody>
</table>
2. Perceptions about internal audit’s level of information security expertise
3. The frequency with which internal audit reviews various aspects of information security

The importance of internal audit’s perceived level of information security expertise and the frequency of audit reviews were corroborated in a follow-up survey study.

**Perceived Role of Internal Audit**

In the interviews, information security professionals indicated that how internal auditors approached the review of information security profoundly affected the quality of the relationship. At one extreme, the auditors could be perceived as “the police” who were out to catch mistakes; at the other extreme, they could be viewed as consultants or advisors. Not surprisingly, the two examples had markedly different effects on the quality of the relationship. When auditors were viewed as “the police,” the relationship was formal, reserved and even adversarial; but, when auditors were perceived more as advisors and consultants, the relationship was more open and positive. The latter view was most clearly explained by the information security manager who provided the comment about the “cat-and-mouse” game quoted earlier, who said: “We can leverage each other’s expertise and position in the organization to make things happen. Many times the IT department will tend to almost hide things from audit because they do not want to get a black eye and we don’t have that issue here so much…we have the same goals.” An information systems professional at another institution expressed a similar comment, saying, “[Our relationship is] exceptionally strong to the point that we’ve just realized we have a codependent relationship. It’s been very positive.” These positive comments are related to the issue of trust. As the information security manager interviewed who talked about the typical “cat-and-mouse” relationship said, “I trust that [the internal auditor is] not out to catch anybody doing anything. He’s out to identify and reduce risk.”

However, when attempting to build a good relationship, auditors must be careful not to imperil their objectivity and independence. Moreover, it may be almost inevitable that when auditors are the bearers of bad news in the form of audit findings, they will be viewed as compliance monitors or “the police.” Indeed, respondents to the survey indicated that they saw internal auditors as both monitors and advisors. Consequently, this may be why the survey results did not find a statistically significant relationship between perceptions of audit’s role and the quality of the IT-to-audit relationship. However, the interview data support the argument that auditors should strive not to be perceived as enforcement officers.

---

**Figure 2—Determinants and Outcomes of Relationship Between Internal Audit and Information Security**

- **Perceived Role of Internal Audit**
- **Internal Audit’s Level of Information Security Knowledge**
- **Frequency of Audit Reviews of Information Security**
- **Relationship Quality (Audit-Information Security)**
- **Perceived Value Added by Internal Audit**
- **Information Security Effectiveness**

©2014 ISACA. All rights reserved. www.isaca.org
Not surprisingly, the key factor may be the attitudes of the heads of both functions. As one information security manager stated, “… the executive auditor gets along with our vice president of IT really well, and they understand—again, they don’t just look at one task, they see the whole picture. That’s the most important thing from the workforce point of view. When they see that demonstrated up high, that’s how they follow suit. They watch this, and then they know that’s the expectation and it’s pretty effortless here. People partner and just get along well with the same goal in mind. It shows.”

To capture the information security participants’ view of the role of internal audit in their organizations, participants were asked to rate internal audit’s role in three categories as shown in Figure 3.

As indicated in Figure 2, participants did not perceive the role of internal audit to significantly impact the overall relationship between information security and internal audit. However, the perception of internal audit’s technical expertise has a significant impact on the quality of the relationship.

In the interviews, IS professionals repeatedly made comments about the importance of internal auditors possessing technical knowledge. For example, one respondent commented, “We’ve actually been very fortunate to hire a very competent IT internal auditor, intimately familiar with ITGC… That’s been really positive. And he’s very technical so that’s a big advantage. Many auditors that I have worked with in the past are not as technical. When [the internal auditor] goes on vacation, I sure am glad to have him return.”

In contrast, the chief information security officer (CISO) at another institution where internal audit did not have much technical skill said, “We see them and we have a very good working relationship with internal audit. However, their focus is typically auditing business processes. You know, ‘are things being done right in payroll?’, and ‘are we handling travel vouchers right?’” Although the CISO stated that the relationship was positive, the overall tenor of the interview indicated that it was really more a case of being nonadversarial than collaborative.

Respondents to the survey corroborated the importance of internal audit possessing strong technical skills, in particular, knowledge about information security. The survey instrument asked information security professionals whether they thought that internal auditors in their organization were “knowledgeable about information security” and whether they kept their “knowledge about information security current” (see Figure 4). Higher scores on these two questions were significantly related to more positive views about the quality of the relationship between the two functions.

Taken together, the interviews and the survey clearly indicate that auditors’ technical expertise fosters a good relationship with the auditee (information security).

Frequency of Audit Reviews of Information Security
It is hard to develop a good relationship unless there is fairly frequent interaction. In the context of the relationship between the internal audit and information security functions, the most likely form of interaction involves audit reviews.
However, audit reviews of information security are affected by internal audit’s level of technical expertise, making it difficult to distinguish between the frequency of review and expertise factors in the interviews. For example, the previously quoted CISO who stated that he had a positive relationship with internal audit, but that they focused on business processes (e.g., fraud prevention), also indicated that he did not think the internal auditors in his organization possessed much technical expertise (and the auditor interviewed at that same organization agreed).

In addition to questions about internal audit’s level of information security expertise, the survey instrument also asked questions about the frequency of internal audit reviews of eight aspects of information security (figure 5).

**Figure 5—Internal Audit Reviews of Information Security Topics**

<table>
<thead>
<tr>
<th>Information Security Topics</th>
<th>Mean (Median)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business continuity and disaster recovery</td>
<td>2.72 (3.0)</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>3.17 (3.0)</td>
</tr>
<tr>
<td>Logging and system monitoring</td>
<td>3.00 (3.0)</td>
</tr>
<tr>
<td>Firewalls and other network access devices</td>
<td>2.56 (3.0)</td>
</tr>
<tr>
<td>Encryption policies (including key management)</td>
<td>2.28 (2.0)</td>
</tr>
<tr>
<td>Backup procedures</td>
<td>2.72 (3.0)</td>
</tr>
<tr>
<td>Change management controls</td>
<td>3.00 (3.0)</td>
</tr>
<tr>
<td>Security policies</td>
<td>3.28 (3.5)</td>
</tr>
</tbody>
</table>

Mean and median responses for all aspects were three on a scale of one to five, with one being “not at all” and five representing “often.” The responses ranged across the entire spectrum. Statistical analysis revealed that there was a significant positive relationship between frequency of audit reviews of those eight areas and the overall quality of the relationship between the information security and internal audit functions. Therefore, more frequent interaction in the form of audit reviews improves the relationship. However, the mean and median scores indicate that there is room for further improvement.

**BENEFITS FROM A GOOD RELATIONSHIP BETWEEN INTERNAL AUDIT AND INFORMATION SECURITY**

Some of the factors that affect the relationship between the internal audit and information security functions have been discussed. Those factors are clearly items that can be improved by managerial action, for example:

- The leaders of both functions can make an effort to develop a positive relationship.
- Additional resources can be invested to increase internal audit’s technical expertise in matters related to information security.
- Increases in the audit budget can enable more frequent audit reviews of information security.

Nevertheless, such investments are worthwhile only if improving the quality of the relationship between internal audit and information security produces tangible benefits. Figure 2 indicates that it does—better relationships improve perceptions about internal audit’s value as well as the overall effectiveness of information security.

**PERCEIVED VALUE-ADD FROM INTERNAL AUDIT**

In the interviews, information security professionals indicated that a positive relationship improved their perceptions about the value added by internal audit. One reason is that information security professionals believe a good relationship with internal audit makes it easier for them to persuade employees and management to support information security initiatives. For example, one CISO stated, “The relationship with internal audit has been very positive…a real big benefit to us achieving a lot of the goals we have from an information security perspective.” The CISO goes on to explain that he feels he can use the audit findings to his advantage, “…and we are going to begin reinforcing the importance of change control. And more importantly, the importance of completed documentation as part of change control for the deployment of new services; and we are going to strongly reinforce through internal audit reports.” The information security manager at another organization described the benefits of a good relationship in obtaining compliance, “If I am just being the IT network police, and I have to get [the internal auditor] and he goes in there with a suit and says ‘here is why you do not want to do this,’ they just usually put their tails between their legs.”

Figure 6 shows the questions used to evaluate the quality of the relationship between internal audit and information security. As with the other questions in the survey, responses ranged from strongly disagree (1) to strongly agree (5).
The higher respondents rated the quality of the relationship between the internal audit and information security functions, the more they agreed with questions about whether the information security professional thought that internal audit findings/reports provided useful information to the information security function and whether internal audit’s capability to review information was being fully utilized.

Figure 6—Perceived Quality of the Relationship Between Internal Audit and Information Security
Respondents were asked to respond on a scale from “strongly agree” to “strongly disagree” to the following statements:
1. In my organization, there is little friction between internal audit and information security.
2. In my organization, the relationship between internal audit and information security staff is close and personal.
3. In my organization, there is a good working relationship between internal audit and information security.

Figure 7—Perceptions of the Value Added by Internal Audit
Respondents were asked to respond on a scale from “strongly agree” to “strongly disagree” to the following statements:
1. In my organization, internal audit findings/reports provide useful information to the information security function.
2. In my organization, internal audit findings/reports provide useful information to top management about the effectiveness of information security. (Dropped from final model)
3. In my organization, internal audit capability to review information security is fully utilized now.
4. In my organization, internal audit could be more involved in reviewing information security.
5. In my organization, internal audit should be more involved in reviewing information security.

Figure 8—Effectiveness of Information Security
Respondents were asked to respond on a scale from “strongly agree” to “strongly disagree” to the following statements:
1. Over the past three years, in my organization the number of information security incidents that have either interrupted operations or resulted in financial loss has declined.
2. Over the past three years, in my organization the overall effectiveness of information security has increased.
3. Over the past three years, in my organization the number of internal audit findings that relate to information security has decreased.

CONCLUSION
COBIT® 5 acknowledges the importance of cross-functional collaboration to achieving effective governance and management of enterprise IT (GEIT).20, 21 In particular, the internal audit and information security functions can synergistically work together to optimize the overall effectiveness of information security.

Yet in practice, these two functions do not always have a harmonious relationship. Therefore, a multistudy program of research was conducted to investigate the factors that affect the quality of the relationship between these two important functions and the benefits associated with having a positive relationship. This article reported the perspectives of information security professionals about those issues. A subsequent article will look at these questions from the viewpoint of internal auditors and is planned for publication in volume 3, 2014, of the ISACA Journal.
ENDNOTES

6 Op cit, Steinbart et al., 2012
9 Op cit, Steinbart et al., 2012
10 Ibid.
11 Ibid.
14 Op cit, Steinbart et al., 2012
15 Ibid.
16 Ibid.
17 Ibid.
19 Institute of Internal Auditors, Change and Patch Management Controls: Critical for Organizational Success 2nd Edition, USA, 2005
20 ISACA, COBIT 5, USA, 2013, p. 29 and 80, www.isaca.org/cobit
21 ISACA, COBIT 5 Implementation, USA, 2012, p. 72, www.isaca.org/cobit