GOVERNANCE GAINS

DIGITAL GOVERNANCE

CONNECTING GOOD GOVERNANCE WITH KEY RISK

CASE STUDY—BUILDING AN ENTERPRISE SECURITY PROGRAM
Train. Test. Protect.

Prove you have the critical skills to defend your organization against cyber threats with the only comprehensive, true-performance cyber certification—ISACA’s CSX® Cybersecurity Practitioner.*

Build your technical cybersecurity skills from anywhere online, on demand in CSX’s unique live, dynamic network environment. The virtual environment’s real-time feedback allows practitioners to immediately identify areas in which they need more focus.

www.isaca.org/OnlineLearning-jv4

*ISACA’s CSX® Cybersecurity Practitioner (CSX-P) certification was named 2016 Top Professional Certification program by the SC Magazine Awards.

ISACA®, the Cybersecurity Nexus™ (CSX) mark, and ISACA’s Cybersecurity Nexus™ (CSX) products, certifications, and services are not affiliated with CSX Corporation or its subsidiaries, including CSX Transportation, Inc.
Keep Learning

Get the training (and CPEs) you want, anywhere you want it, with ISACA®’s online training solutions. Choose from training options for individuals and groups.

www.isaca.org/OnlineLearning-jv4
The ISACA® Journal seeks to enhance the proficiency and competitive advantage of its international readership by providing managerial and technical guidance from experienced global authors. The Journal’s noncommercial, peer-reviewed articles focus on topics critical to professionals involved in IT audit, governance, security, privacy and assurance.

Read more from these Journal authors...

Journal authors are now blogging at www.isaca.org/blog. Visit the ISACA Journal blog, Practically Speaking, to gain practical knowledge from colleagues and to participate in the growing ISACA® community.

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Telephone +1.847.660.5505
Fax: +1.847.253.1755
www.isaca.org
Privacy by Implementation and Execution

When I was in graduate school, I read a lot of scholarly journals. (None of them were as lively nor as useful as the journal you are now reading.) One of the features I loved best was a rousing argument between academics about matters of miniscule interest to the general public. The articles, letters, counterarticles and counterletters were full of high dudgeon, *ad hominem* attacks and general rapscalliousness.

A few issues back in the ISACA® Journal, I published two articles about data privacy.¹,² They expressed my skepticism that current privacy laws, especially the EU General Data Protection Regulation (GDPR), would accomplish their stated aims, with particular focus on the concept of “privacy by design.” Not for the first time, I staked out a contrarian position in hopes of stirring up some controversy.

And controversy I got. In a subsequent issue of this Journal, Mr. Ian Cooke begged to differ.³ (You can meet Mr. Cooke a few pages hence, as he, too, is a columnist here.) I want to point out first that Mr. Cooke is in very low dudgeon, is respectful throughout his reply and is in no sense a rapscallion.⁴ I will offer my ripostes in the same spirit.

Replying to Comments

I had said that “data privacy laws should be focused on cases of actual harm.”⁵ Mr. Cooke points out that Facebook is accused of causing genuine harm by “restricting who can view housing-related ads based on their ‘race, colour, national origin, religion,’”⁶ which are sensitive personal data under GDPR. We are in complete agreement, and that sort of misuse of personally identifiable information (PII) is the theme of my second article about organizations that design un-privacy⁷ into their systems. I believe and I have stated that we will achieve greater data privacy across society if we focus attention on breaches that hurt people and not on violations of process and protocol.

I directed some disdain at the inscrutable prose in the “Privacy by Design” section of GDPR⁸ and stated that it was clearly written by a committee. Mr. Cooke rises to the defense of laws written by multiple representatives. My objection is not to writing groups, as such, but to the type of incomprehensible verbiage that they often produce. I am not the first to note that a camel is a horse put together by a committee. On this issue, alas, I believe Mr. Cooke and I fated to disagree.

Most importantly, Mr. Cooke examines whether cyberattacks that resulted in privacy breaches are caused by a failure of design. Here our difference of opinion is foundational and worth exploring in further depth.

Cyberattacks, Privacy and Risk Assessment

I mentioned several such attacks in one of my articles, one of which was the massive breach at Equifax.⁹ I do find it shocking that a company that is

---

Steven J. Ross, CISA, AFBCI, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the Journal’s most popular columns since 1998. He can be reached at stross@riskmastersintl.com.
in the PII business could be so lax. But were their systems poorly designed in terms of protecting the information in their trust? According to press reports, a good case could be made, inasmuch as Equifax had experienced several successful cyberattacks in the previous year.¹⁰

But without getting into the particulars of this case, about which I have no personal knowledge, let us ask the broader question: Are successful cyberattacks indicative of poor privacy and security design? Based on my experience, I think not. No organization that I have dealt with sets out to have inadequate security. The fact that their security proves to be deficient is often based on a shortfall in risk assessment.

It is well understood that organizations should evaluate the risk to their information resources and apply suitable controls consistent with their understanding of the potential for those resources to be misused. But sadly, there may be a gap between the assessment and the reality. Assessments are extrapolations of known facts into potential outcomes. To the extent that imprecision leads to error, these organizations find themselves exposed.

Banks know that their information is valuable and at risk. So does the military. Yet banks have been severely attacked¹¹ and so have military systems.¹² Surely no one thinks that organizations such as these are incapable of designing security—and by extension privacy—into their systems. Someone was simply able to exploit a shortcoming that a risk assessment did not and could not identify in advance.

Implementation and Execution

Ah, I can hear Mr. Cooke asking me, but how did those weaknesses get there? And I would answer, should he ask, that security was designed properly but not implemented well. And even then, complete implementation of security is impossible. No matter how well an organization’s systems are designed and implemented, they run on operating systems and other infrastructure in which flaws are identified daily. If there were to be a zero-day attack, how could any organization be faulted for failing to anticipate and prevent it?

Even if perfect implementation were possible, perfect execution cannot be, because execution relies on fallible human beings. Security systems that undergird privacy will never be foolproof because the world contains too many fools. Yes, an organization could design systems that anticipate dumb people doing dumb things, but too many breaches are due to the failings of otherwise smart people. And that is not to mention the unscrupulous and avaricious among us. Errors will occur and personal information will be disclosed because of failures of trust as well as deficiencies of security.

Time Pressure

As I wrote in the Un-Privacy article, it is the exigencies of the market that lead to poor privacy over personal information. There is tremendous pressure to get software to the market as quickly as possible. As it is, too much software is delivered that does not do what it is supposed to do; it is probably too much to ask that it not do what it is not supposed to do, that is, disclose PII.

It is not only commercial software that makes privacy by design difficult to implement and execute. Agile development, so popular these days, creates challenges in complying with GDPR and other privacy requirements. In my opinion, Agile undervalues documentation, which makes it difficult for auditors and privacy specialists to determine whether and how privacy has been designed into a system.¹³ While I am not saying that Agile is the enemy of privacy, I do believe that it is one more factor that mitigates against implementing adequate privacy in system development.

So, Mr. Cooke, we both agree that privacy by design is an admirable objective. Everybody ought to do it, but then everyone also ought to live in virtue and abhor sin. I am in favor of both privacy and virtue, but I remain dubious about their achievement.
Ian Cooke Responds

I would like to thank Mr. Ross for his thoughtful and respectful column. However, if privacy and, indeed, virtue are admirable objectives, are they not something to which we should aspire? We should at least try. And we can only do this by design.

Endnotes

4 Each of us submits our articles four months before they are published, so this conversation is occurring in slow motion, although Mr. Cooke and I did speak in March 2020.
5 Op cit Ross, 2019, “Why Do We Need Data Privacy Laws?”
6 Op cit Cooke
7 This is a neologism if ever there was one, but it suits the purpose. If it is not a proper English word, it ought to be. It’s my word and I’m sticking with it.
10 Ibid.
Earlier this year, I authored a column on the “Components of an IT Audit Report.” These components need to provide assurance, inform auditees and others of management and control issues, recommend corrective action, and represent the quality of the audit and the credibility of the audit organization. How the audit report is organized and written can significantly impact these objectives. A logical follow-up question to this column would, therefore, be what would the actual contents of these components look like? Particularly, what would the “Findings, Conclusions and Recommendations” and the “Executive Summary” components look like?

Setting the (COBIT 2019) Scene

Before discussing these components further, it is worth recapping some COBIT® 2019 concepts, as these will be referenced later.

Enterprises can have different strategies, which can be expressed as one or more of the archetypes shown in figure 1. Organizations typically have a primary strategy and, at most, one secondary strategy. These strategies are realized by the achievements of enterprise goals (figure 2). In turn, alignment goals (figure 3) emphasize the alignment of all IT efforts with business objectives. The alignment goals, in turn, drive the governance and management objectives (COBIT® processes) (figure 4).

Findings, Conclusions and Recommendations

In my previous column, I shared a figure on the five attributes of an audit finding (figure 5). I am now proposing that these attributes can be derived from the components of the goals cascade (figure 6).

The following is a sample internal audit finding applying the method while also referencing another useful resource for audit reports, the ISACA® Glossary.

Sample Internal Audit Finding: Disaster Recovery

A disaster recovery plan (DRP) refers to the set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster.

Our audit disclosed that the company would be unable to recover its sales order processing (SOP) system in line with business requirements (figure 3 AG05) should the primary processing facility be rendered inoperable. Although replication is in place between the primary and secondary facilities, recovery strategies for different disaster scenarios have not been developed and documented in a DRP. Further, no disaster recovery tests have been performed. The IT-related risk is, therefore, not being adequately managed (figure 3 AG02) (figure 5 Condition).
### Figure 1—Enterprise Strategy Design Factor

<table>
<thead>
<tr>
<th>Strategy Archetype</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Growth/acquisition</td>
<td>The enterprise has a focus on growing (revenues).</td>
</tr>
<tr>
<td>Innovation/differentiation</td>
<td>The enterprise has a focus on offering different and/or innovative products and services to their clients.</td>
</tr>
<tr>
<td>Cost leadership</td>
<td>The enterprise has a focus on short-term cost minimization.</td>
</tr>
<tr>
<td>Client service/stability</td>
<td>The enterprise has a focus on providing stable and client-oriented service.</td>
</tr>
</tbody>
</table>

Source: ISACA®, COBIT® 2019 Introduction and Methodology, USA, 2018

### Figure 2—Enterprise Goals

<table>
<thead>
<tr>
<th>Reference</th>
<th>Enterprise Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>EG01</td>
<td>Portfolio of competitive products and services</td>
</tr>
<tr>
<td>EG02</td>
<td>Managed business risk</td>
</tr>
<tr>
<td>EG03</td>
<td>Compliance with external laws and regulations</td>
</tr>
<tr>
<td>EG04</td>
<td>Quality of financial information</td>
</tr>
<tr>
<td>EG05</td>
<td>Customer-oriented service culture</td>
</tr>
<tr>
<td>EG06</td>
<td>Business-service continuity and availability</td>
</tr>
<tr>
<td>EG07</td>
<td>Quality of management information</td>
</tr>
<tr>
<td>EG08</td>
<td>Optimization of internal business process functionality</td>
</tr>
<tr>
<td>EG09</td>
<td>Optimization of business process costs</td>
</tr>
<tr>
<td>EG10</td>
<td>Staff skills, motivation and productivity</td>
</tr>
<tr>
<td>EG11</td>
<td>Compliance with internal policies</td>
</tr>
<tr>
<td>EG12</td>
<td>Managed digital transformation programs</td>
</tr>
<tr>
<td>EG13</td>
<td>Product and business innovation</td>
</tr>
</tbody>
</table>

Source: Modified from ISACA, COBIT® 2019 Introduction and Methodology, USA, 2018

### Figure 3—Alignment Goals

<table>
<thead>
<tr>
<th>Reference</th>
<th>Alignment Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG01</td>
<td>I&amp;T compliance and support for business compliance with external laws and regulations</td>
</tr>
<tr>
<td>AG02</td>
<td>Managed I&amp;T-related risk</td>
</tr>
<tr>
<td>AG03</td>
<td>Realized benefits from I&amp;T-enabled investments and services portfolio</td>
</tr>
<tr>
<td>AG04</td>
<td>Quality of technology-related financial information</td>
</tr>
<tr>
<td>AG05</td>
<td>Delivery of I&amp;T services in line with business requirements</td>
</tr>
<tr>
<td>AG06</td>
<td>Agility to turn business requirements into operational solutions</td>
</tr>
<tr>
<td>AG07</td>
<td>Security of information, processing infrastructure and applications, and privacy</td>
</tr>
<tr>
<td>AG08</td>
<td>Enabling and supporting business processes by integrating applications and technology</td>
</tr>
<tr>
<td>AG09</td>
<td>Delivery of programs on time, on budget, and meeting requirements and quality standards</td>
</tr>
<tr>
<td>AG10</td>
<td>Quality of I&amp;T management information</td>
</tr>
<tr>
<td>AG11</td>
<td>I&amp;T compliance with internal policies</td>
</tr>
<tr>
<td>AG12</td>
<td>Competent and motivated staff with mutual understanding of technology and business</td>
</tr>
<tr>
<td>AG13</td>
<td>Knowledge, expertise and initiatives for business innovation</td>
</tr>
</tbody>
</table>

Source: Modified from ISACA, COBIT® 2019 Introduction and Methodology, USA, 2018
**Figure 4—COBIT Goals Cascade**

- **Stakeholder Drivers and Needs**
- **Enterprise Goals**
- **Alignment Goals**
- **Governance and Management Objectives**

Source: ISACA, COBIT® 2019 Introduction and Methodology, USA, 2018

**Figure 5—Five Attributes of an Audit Finding**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Identifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>Findings</td>
<td>The auditor findings. It is a statement of the problem or deficiency. This may be in terms such as control weaknesses, operational problems, or noncompliance with management or legal requirements.</td>
</tr>
<tr>
<td>Criteria</td>
<td>Requirements and baseline</td>
<td>Statement of requirements and identification of the baseline that was used for comparison against the auditor findings, based on the audit evidence.</td>
</tr>
<tr>
<td>Cause</td>
<td>Reason for the condition</td>
<td>While the explanation of the cause may require the identification of the responsible party, it is suggested that, unless required by audit policy, the report should identify the organizational business unit or person's title and not the individual's name. The same should be applied to the identification of the person representing the relevant point of accountability.</td>
</tr>
<tr>
<td>Effect</td>
<td>Impact of the condition</td>
<td>The answer to the question “so what?” It explains the adverse impact to the operational or control objective. By articulating impact and risk, the element of effect is very important in helping to persuade auditee management to take corrective action.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Suggested corrective action</td>
<td>While the corrective action should eliminate the problem or deficiency noted in the condition, the corrective action should be directed toward addressing the cause.</td>
</tr>
</tbody>
</table>

Source: ISACA, IS Audit Reporting, USA, 2015

**Figure 6—Attribute to Goals Cascade Mapping**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Relationship to Goals Cascade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>Finding</td>
<td>Failure to achieve alignment goal</td>
</tr>
<tr>
<td>Criteria</td>
<td>Requirements and baseline</td>
<td>Governance and Management Objectives (COBIT or others)</td>
</tr>
<tr>
<td>Cause</td>
<td>Reason for the condition</td>
<td>Why we failed to achieve the alignment goal</td>
</tr>
<tr>
<td>Effect</td>
<td>Impact of the condition</td>
<td>Failure to achieve enterprise goal</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Suggested corrective action</td>
<td>Governance and Management Objectives (COBIT or others)</td>
</tr>
</tbody>
</table>

Enjoying this article?

- Learn more about, discuss and collaborate on audit and assurance ISACA’s Online Forums. https://engage.isaca.org/online-forums
Depending on the nature and extent of loss of the primary processing capabilities, the company would not be in a position to ensure business service continuity and availability (figure 2 EG06) for the application affecting the customer-oriented service (figure 2 EG05) and the quality of management information (figure 2 EG07). This would likely result in an adverse financial impact affecting the enterprise’s growth strategy (archetype) (figure 5 Effect or Impact).

The company needs to implement a DRP for the SOP system in line with the business continuity response. This should document all procedures necessary for the enterprise to continue critical activities in the event of an incident (COBIT Deliver, Service and Support [DSS] DSS04.03). Further, this should be tested on a regular basis against predetermined outcomes (COBIT DSS04.04) (figure 5 Criteria).

While management acknowledged that disaster recovery was important, responsibility to ensure that the SOP system was maintained in line with business requirements (figure 3 AG05) had not been assigned. We also found that the risk management process did not formally consider the loss of IT capabilities (figure 3 AG02) (figure 5 Cause).

Sample Recommendations
We recommend that the company should:

- Identify key stakeholders and roles and responsibilities for defining and developing the DRP
- Develop and maintain operational DRPs that contain the procedures to be followed to enable continued operation of the SOP system
- Define objectives for exercising and testing the plan to verify completeness of the DRP in meeting business risk. This should include input from risk management
- On a regular basis, review the plans to consider the impact of new or major changes to the organization, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and SOP system
- Ensure that management and staff are adequately trained to effectively execute disaster recovery tasks and activities

(All based on COBIT DSS04.)

The report’s executive summary should then be based upon the effect or impact while also summarizing the recommendations.

Some Points to Note
Although already comprehensive, there is no reason why an enterprise should not add to the archetypes, enterprise goals or the alignment goals if they give greater direction or clarity to the organization. Further, even if an enterprise does not use COBIT, the goals cascade can still be implemented as each of the management practices map to other related guidance, for example, the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Information Security Management Systems Requirements, International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27001:2013 and the Center for Internet Security (CIS) Critical Security Controls.

Conclusion
Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. There is no better way for internal audit to demonstrate and for senior management to see this value than by directly linking audit report findings to the enterprise’s strategy. Further, the alignment and/or enterprise goals can be captured and measured as part of the audit follow-up process.

Endnotes
Train and Certify—
Then Apply Two Globally Adopted Frameworks to Create Flexible Cybersecurity Governance

Validate your knowledge of how to integrate cybersecurity standards and enterprise governance of information and technology (EGIT) to secure your organization, and your future. Study and certify from anywhere.

Learn more about the Implementing the NIST Cybersecurity Framework Using COBIT 2019 certificate program.

www.isaca.org/COBITNIST-jv4
I have been a remote worker for approximately five years. The transition was not an easy one. However, in the past two years I have come to a very “Zen” place in my work-from-home routine...or lack thereof. Yes, it took me three years to acclimate to the change in work pace, peer socialization and, of course, the technology that enables it. Most of the difficulty in acclimation was due to a psychological shift on my part. The need to push my square-shaped idea of what a job was into the round hole of remote work tested my mental flexibility. But this is an understandable lack of fluidity. I have had a job, at least on a part-time basis, since I was 14 years old and, once I started my full-time career, the 40-hour minimum, 9-to-5, Monday-through-Friday ideology was firmly ingrained in my psyche. Change takes time—unless you do not have the luxury of time.

With the recent global pandemic, many organizations and their employees were faced with the difficult task of transitioning to remote work, where possible, and I have to say I am incredibly impressed with the speed and agility with which this has happened as far as the technology goes. Seemingly overnight, meetings were shifted to digital video conferencing platforms, collaborative cloud platforms were being truly utilized, and, for some, productivity did not skip a beat and perhaps even increased. The truly amazing thing is that this was not just a quick shift in our collective way of work but also our way of personal life and socialization. Perhaps you have been to at least one social event hosted on Zoom. So, let’s look at one of the technologies that allowed this change to happen so quickly. To find the answer, all you have to do is look to the skies.

No Computer Is an Island Unto Itself

If you looked up and saw a cloud, you found the answer. Also, how great that you are outside reading the ISACA® Journal. Enjoy!

It can be argued that the cloud is not an emerging technology. Some argue that it has been here all along or at least since the conception of ARPANET in the 1960s, while others say that “true” cloud computing was first introduced in 2006 by Google's chief executive officer (CEO) at the time, Eric Schmidt. The cloud as we know it today is an immense collection of interconnected systems with hundreds of petabytes of data being stored, processed and transferred. We have also seen massive adoption of this technology within the last decade. Nearly 90 percent of enterprises have already adopted cloud technologies in some form according to Flexera's 2019 State of Cloud Computing. However, the capabilities and

Dustin Brewer, CISM, CSX-P, CDPSE, CCSP, CEH

Is ISACA’s principal futurist, a role in which he explores and produces content for the ISACA® community on the utilization benefits and possible threats to current infrastructure posed by emerging technologies. He has 17 years of experience in the IT field, beginning with networks, programming and hardware specialization. He excelled in cybersecurity while serving in the US military and, later, as an independent contractor and lead developer for defense contract agencies, he specialized in computer networking security, penetration testing, and training for various US Department of Defense (DoD) and commercial entities. Brewer can be reached at futures@isaca.org.
technologies that host the cloud are in a constant state of discovery and implementation and, in that sense, I would postulate that the cloud will remain an emerging technology until it is replaced or is rolled into the next “big thing.” Also, considering this technology was/is a big player in saving a great number of jobs and providing computing power and data infrastructure to researchers investigating possible drugs and vaccines for COVID-19 treatment and prevention, it deserves a second look.

The pre-existing elasticity and capabilities of cloud collaboration tools offered the perfect virtual environment to meet the sudden growth in need for remote productivity. Google initially reported a 60 percent increase in use of its Meet platform at the start of the COVID-19 pandemic.3 In March, Microsoft saw a 775 percent increase in use of its Teams meetings solution in Italy after the Italian government’s social distancing and shelter in place guidelines were established.4 These are staggering numbers, and it is perhaps even more impressive that the service providers were able to handle that kind of influx. Other service providers, such as Amazon Web Services (AWS), have not published usage statistics as of the date of this writing. You do not have to be a futurist to predict that this trend will continue for the foreseeable future as more organizations discover the benefits of remote work.

The cloud has been an enabler for other emerging technologies as well. The Internet of Things (IoT) and artificial intelligence (AI) utilize cloud services on the back end. Serverless functionality is an up-and-coming player in a plethora of applications. Even some blockchain implementations utilize the cloud. If you read my column in the ISACA Journal vol. 3, 2020,5 you would know that I have a particular passion for the interoperability of emerging tech for which the cloud is a paramount player. And, although this technology is such a big player in our day-to-day lives, we still have issues with security, management and governance of the cloud.

**Wrangling a Cloud**

One of my favorite quotes about the cloud is, “There is no cloud, it’s just someone else’s computer.” While I know this is not 100 percent accurate, it does help my mind wrap around the immensity and complexity of cloud computing and makes the task of securing and governing such systems a little less daunting. Following this train of thought, let’s look at what “someone else’s computer” looks like.

Numerous sources proclaim that Linux makes up the majority of the cloud (up to 90 percent). For some reason, this skill set still eludes some IT and cybersecurity professionals. Possibly because a large number of enterprises utilized Microsoft products. But Microsoft is changing its once negative tone on Linux and even embracing it with Windows Subsystem for Linux and utilizing Android for its upcoming smartphone. Microsoft also admits that almost half of its Azure instances are running Linux distributions.6 Depending on your cloud service type (i.e., Software as a Service [SaaS], Platform as a Service [PaaS], Infrastructure as a Service [IaaS]), you may not need to worry about security and governance at this granular level, but understanding the underlying operating system (OS) can still be key to understanding mitigation and compliance. As an added bonus, it can also aid in understanding some IoT security issues.

On a higher level, we can turn to frameworks. Current cloud-specific guidance can be found via the US National Institute for Standards and Technology (NIST) Special Publication (SP) SP 500 series as well as International Organization for Standardization (ISO) ISO 27017, but guidance is not limited to cloud-specific documents. Recently, I collaborated on specific guidance for governing and securing remote working already present in COBIT® 2019, which can be applied to certain aspects of cloud usage.7 The NIST Cybersecurity Framework (CSF) is also a good place to start with any information technology system. However,
frameworks are just a set of guidelines and best practices. It is up to the professional to be flexible with her or his use of these tools and the enterprise’s specific use cases, especially when it comes to emerging technologies.

One of the more challenging aspects can be that a lot of the security responsibilities fall on the end users. Education and culture play a large role in security incident prevention and continual compliance for cloud implementations. This is where we, as professionals in the IT field, can really step up and lead by example. Most of our cloud services are available from anywhere and that is, basically, the point. We tend to let our guards down in the comfort of our own homes, however, it should be emphasized that while accessing enterprise services, the same precautions used in the office should be taken anywhere.

Out of the Clouds

While the cloud and its enabling technologies have played a major role in business continuity during this global crisis, there have been some pitfalls. Security and privacy continue to be an issue and, in some cases, so does stability. As professionals mostly concerned about security, privacy and stability, these can seem like big problems, and they can be, depending on the severity and breadth. But if we can take a step back and look holistically at the evolution of the cloud, it is hard not to be impressed with the virtual world that we have built. It provided and is still providing a haven where we can continue to work (and play) even in some of the worst circumstances. The cloud allows us to continue to engage, socialize and produce, keeping our spirits up and demonstrating that, even in the darkest of times, there may yet be blue skies ahead.

Endnotes

Responding to a Changing Business Landscape

Q: As ISACA’s incoming chair of the Board of Directors, how do you see ISACA® growing and adapting to the constantly changing marketplace and needs of its constituents over the next year?

A: That is a good question. Since I joined the board, we have been focused on putting ISACA in the best position to continue to be a leader in its space. We have been laying the groundwork that will enable us to react more quickly to a constantly changing marketplace. We have added a number of people to the board who have significant business experience and experience in strategy; we have a new management team with deep experience in learning and development; we are investing in our infrastructure in the form of new technology; we are conducting new training internally and adopting an agile work environment.

Next, we will be focusing on acquiring the data we need to determine where and what our membership and the marketplace want and need. We have all talked about how we can engage younger people in our organization, gain more diversity and expand our global footprint, but we have never had solid data from which to make good decisions. We receive a lot of data from the chapters, but truthfully, the majority of the membership does not engage in the chapter model, so we are losing input from a great number of our constituency. This means we have to find ways to access the full membership for data. We receive a lot of data from the chapters, but truthfully, the majority of the membership does not engage in the chapter model, so we are losing input from a great number of our constituency. This means we have to find ways to access the full membership for data. Further, we need data from the people we wish to engage with, such as the younger generations. Once we have the data, we will figure out how we can “win” in the marketplace and deliver value to the organization.

Q: What in your past experience has best prepared you for this position on the ISACA Board?

A: I have C-suite experience in taking organizations that are operating suboptimally and fixing them based upon a lifetime of experience in strategy, risk and compliance, finance, capital markets, investor relations, regulatory management, and crisis management. My experience ranges from working in Fortune 50 companies to small private institutions. All of these experiences are relevant to this organization.

Q: What do you see as the biggest risk factors being addressed by ISACA constituents?

A: As a board member listening at chapters’ events, I can tell you that I worry about the seeming inability of the membership to communicate effectively to the people above them about the needs and risk within the organization. A large part of what ISACA does is provide the technical skills members need to progress in their careers, and most of our members are in middle management. They are in areas that are critical to the organization but are not revenue producing, and they do not have a seat at the table with management. As a result, they do not feel that they get the time, attention and resources they need to ensure the safety and security of the enterprise. I hear this lament a lot. We all know information security can be highly technical and the devil is in the details. Those at the top are not...
generally technology experts, so it is often a matter of finding a way to communicate in a manner in which executive leadership can understand and absorb. Communicating effectively is equally as important as what you know.

Q: You have extensive experience in executive leadership. How do you see the role of executives changing to meet the challenges of information security?

A: Carrying on a theme that Brennan Baybeck put forward as incoming Board Chair last year, having good information security is now table stakes. Enough chief executive officers (CEOs) have lost their jobs and shareholder value has been destroyed over information security issues for executives to get the message. Executives are paid to identify, understand and weigh risk and make good choices that lead to shareholder/stakeholder value creation. Today, this often means making significant changes in the business through digital transformation, the use of blockchain, robotic process automation (RPA), artificial intelligence (AI), big data and the Internet of Things (IoT). Executives need to stay on top of the changing business landscape and the risk scenarios that are created as a result of that rapidly changing landscape. To do that, they need to equip themselves with the ability to ask the right questions, whatever that entails. Two examples are: not being afraid to say “I do not understand, explain it to me;” and hiring the best people you can who are experts in areas in which you are not.

Q: What do you think are the most effective ways to address the skills, gender and diversity gaps in the technology space?

A: Ensure that women and other diverse candidates have role models at all levels across the organization. Organizations are good at having diversity up to a point but, as the pyramid narrows, diverse candidates become very scarce. I was surprised to learn how much it meant to other women in the organization that I had gotten this or that promotion. It gave them hope that it was actually possible for them as well.

Another way to address these gaps is to create education degrees and certifications that fulfill a technical market gap but do not require the full broad education required at institutions of higher learning, and making those affordable. I would also like to see greater efforts to retool the skills of people who have lost their jobs midcareer in an affordable and effective way.

Q: What has been your biggest workplace or career challenge and how did you face it?

A: There have been many “biggest challenges” I have had to face over the years, each one seeming to be the “biggest” at the time it occurred. I would say that when you get to my age, there is little you have not faced, and it is a matter of staying focused and not letting the problem overwhelm. My mantras are: 1. Keep perspective. The challenge may seem overwhelming at the outset, but “This, too, will pass”; 2. Get as much information together as soon as you can about the issue; 3. Prioritize and attack the issue in a thoughtful and organized manner, and it will eventually lead to the changes; 4. Galvanize the troops and make the goal clear so everyone is aligned; and 5. Celebrate all wins.
Leadership expert and former US Navy SEAL Jocko Willink wrote the following, "And most important, discipline will put you on the path to FREEDOM." What does this have to do with innovation? Everything, as it turns out. Discipline, by Willink’s definition, is regularly doing the things you are supposed to be doing. From a military preparedness level, being disciplined gives you a better chance for survival and helps you deal with unexpected situations. It means you exercise when you can, you ensure your gear is ready to go, and you study up and know what you are supposed to be doing when you are supposed to be doing it. By being disciplined, you free yourself to think, to seize new opportunities, to confront the critical. That is what we are doing in innovation.

The key point for anything related to innovation is to help the organization better compete. Therefore, innovation does not want to set the organization back long term. That defeats the purpose of the innovation effort. As a result, innovation should embrace governance throughout the process. This ensures that what comes out of the innovation efforts is useful to the organization and not costly instead. If we were to just stop there, we have a good enough reason to include governance as part of innovation. However, there is more that governance provides for us.

**Governance: An Organization's Safety Net**

The reason we have controls and governance is to protect the organization. We are trying to reduce the risk of a bad process or person. Over time, governance evolves. As technology, people and processes change, so, too, does the governance. It must be adapted to fit the changing conditions. If proper review and revision occur, governance helps protect the organization.

On the other hand, when governance is not properly kept up with, the organization is put at risk. It may even be greater risk than no governance at all. A tangible analogy here comes from the world of sports. Imagine a piece of gear, such as a helmet, with the requisite rules and standards that define what minimum specifications the gear must meet. In order to make things easier, some professional sports organizations will even mandate a list of approved models.

Now, imagine the case where an old model is still approved even though the right testing will show it does not meet what is needed in today’s game. Even worse, the minimum specifications have not been updated. As a result, one helmet on the list of approved gear meets the current standards but does not properly address the current risk to the player. It is likely players wearing such gear will suffer injuries that could have been prevented had the standards and the list of approved helmet models been properly updated. It might even be
possible to argue that by not limiting the models of helmets, teams and players would have chosen better gear. In this case, we have an example where an outdated set of governance controls could potentially result in greater risk.

The reason I make a point about outdated governance is that governance itself is not what impairs innovation. Rather, it is outdated governance that gets in the way of innovation. However, outdated governance is not just a problem for innovation. Rather, it is a risk to the overall organization. Therefore, it should be addressed in that context.

“HAVING PROPER, UPDATED GOVERNANCE MEANS WE CAN FOCUS MORE ON THE INNOVATION EFFORT ITSELF.”

Governance: The Freedom to Hyper Focus

By having proper governance, we know what the rules are in critical areas with respect to the operating environment. We do not have to think about what the rules should be as we are working on something to move the organization forward. The time we do not have to spend thinking about what the rules should be frees us up to be able to innovate. This is the core message behind Willink’s quote that “discipline equals freedom.” Having proper, updated governance means we can focus more on the innovation effort itself.

Often, when writing an article or preparing a talk, it is not unusual to have too much material. Writers and speakers must spend time trying to pare down the material to meet the requirements of the work. The general rule is the shorter the article or talk, the more time will have to be spent to do the cutting. The reason to do the cutting is to ensure that the core message shines through. Everything that could distract from that core message must be cut.

The nature of governance is that it should tell us what is off limits. It tells us what is not core. If there is an area of the market we are not supposed to get into or that is so tightly controlled with regard to particular processes and even specific systems, we know those are areas not to waste time with on the innovation side, as there are likely to be bigger payoffs elsewhere. Therefore, governance helps define our focus, which increases the likelihood that the innovation efforts will pay off.

Governance: Innovation for Other Areas of the Organization

What I have found in years of experience in IT and audit/security is that oftentimes we define a control and, as long as it keeps on working for us, we do not spend time/effort trying to improve it. This is logical, as we would rather spend our resources on moving the needle forward. Only when there is pain around a control do we tend to revisit it.

The great thing about innovation is we are often building new things or implementing things in a new way. In that effort, we get the opportunity to revisit controls. Perhaps a way we are building something in the innovation is applicable to an existing control. For instance, we want to better parse web server log traffic to spot problems before an outage results. In the effort to build this better web server log parser, we also build something that might be applicable to controls around web server monitoring for the organization.

We could also realize something we build to meet governance requirements is applicable somewhere else. For instance, if I need to build a better rights tracking system for a particular application that is considered critical, in the process of building that system I may reveal information that could be used to improve employee on-boarding processes, which can be tossed over to innovation to flesh out.

Enjoying this article?

• Read Rethinking Data Governance and Data Management. www.isaca.org/rethinking-data-governance
• Learn more about, discuss and collaborate on audit and assurance in ISACA’s Online Forums. https://engage.isaca.org/onlineforums
Governance: The Value of Intent

There is an old maxim in chess, “Better to have a bad plan than no plan at all.” The meaning behind the maxim is that it is better to have an understanding of what you are trying to accomplish than be totally lost and just pushing pieces to complete moves. The difference is intent.

Governance, when we understand the intent, gives us business value. It tells us what most needs protecting. It reveals to us where the weak points are located. It lets us know on what we could be working. That is valuable information to an innovation effort.

Not only can governance tell us where we should not waste our time, it can tell us where we should be spending time. If we are looking to maximize the return on investment (ROI) of an innovation effort, that is exactly what we need.

Embracing Governance

Not only can governance keep us from making huge missteps that cost the organization, but it can help innovation efforts. The first thing governance can do is pare down what we can focus on by telling us what should be avoided. Knowing what to cut out of the picture helps tremendously. Second, efforts from innovation can assist governance, but governance efforts themselves can lead to insights on expanding technology and processes outside of the realm of meeting a control to bring more efficiency elsewhere. Finally, by taking the time to understand the governance, the whys behind the controls, we can often better understand what is truly important to the organization and where there are gaps that need filling. That gives us a better idea of where innovation can be put to use.

Endnotes

1 Willink, J.; Discipline Equals Freedom Field Manual, St. Martin’s Press, USA, 2017

NOT ONLY CAN GOVERNANCE TELL US WHERE WE SHOULD NOT WASTE OUR TIME, IT CAN TELL US WHERE WE SHOULD BE SPENDING TIME.

Prepare for Certification Exam Success at Home

Set yourself up for success with ISACA’s official, expert-designed solutions to provide the most comprehensive and up-to-date prep available—online.

www.isaca.org/credentialing-jv4
Never before has there been such an intense focus on digital as during the COVID-19 pandemic. This has been especially true for the business continuity management (BCM) efforts needed to provide work-from-home functionality to support social distancing. Organizations that struggled to action their business continuity plans (BCP) will, in effect, have experienced a digital execution gap (i.e., the difference between the aspirations and the reality of effecting business continuity).

In the same way that a digital gap is experienced in BCP, there is also an enterprise digital strategy execution gap (which incorporates BCP). The following details how governance ensures that the enterprise digital strategy execution gap is as narrow as it can be, ultimately supporting organizational sustainability.

Reinforced by the waterfall model of software development, IT has typically been a reactive enabler of business. The waterfall model begins with business giving IT their requirements, which IT then develops, tests and, ultimately, deploys into production—all in response to the business requirements. The Agile methodology can also be challenged in this, given that it begins with the end user crafting the stories, which are then implemented and deployed either traditionally or in a DevOps paradigm.

A key question is whether reactive IT is sufficient for an organization to sustain its competitiveness and whether strategically proactive IT is becoming a necessity in the interests of organizational sustainability. This key question was introduced in IT-business alignment work and the Strategic Alignment Model (SAM) of 1990. It remains foundational literature for any governance professional, providing a qualified means to frame IT oversight regarding the governance professional’s fiduciary duties on the board.

The first reason for SAM’s continued relevance is in the original article’s title, “Strategic Alignment: A Model for Organizational Transformation via Technology.” An evolution of the article was published in 1999, where the article’s title had become even more interesting: “Strategic Alignment: Leveraging Information Technology for Transforming Organizations.”

Both titles seem appropriate for today’s digital transformation texts because digital transformation is instrumental in organizational transformation, impacting the organization’s operating and

Guy Pearce, CGEIT
Has served on governance boards in banking, financial services and a not-for-profit, and as chief executive officer (CEO) of a financial services organization. He has taken an active role in digital transformation since 1999, experiences which led him to create a digital transformation course for the University of Toronto School of Continuing Studies (Ontario, Canada) in 2019. Consulting in digital transformation and governance, Pearce readily shares more than a decade of experience in data governance and IT governance as an author in numerous publications and as a speaker at conferences. He received the 2019 ISACA® Michael Cangemi Best Author award for contributions to IT governance, and he serves as chief digital transformation officer at Convergence.Tech.

Tony Gaffney, ICD.D
Is a CEO with extensive corporate director experience. He has led and governed enterprises, from small to large (US$3B), through the development and implementation of strategies enabled by technology and digital. His CEO experience includes organizations in the financial, technology, telecommunications, professional and managed services sectors. As a corporate director, Gaffney has served on strategy (chair), technology (chair), human resource (chair), CEO search (chair), special (chair), risk, audit and conduct committees. He is a graduate of the Rotman Corporate Directors program and serves on the advisory board of Convergence.Tech.
Integrating both the operating model, the business model and the customer experience on one hand with the contexts of technology, value creation, structure and financials on the other, a table such as Figure 1 can be created, and it highlights technology’s transformational role.

Another reason for SAM’s sustained relevance is its four perspectives on IT planning:

1. **Technology exploitation**—IT’s influence on business strategy, a concept at the heart of today’s digital transformation paradigm
2. **Technology leverage**—The more traditional understanding of IT’s role, which is how IT supports and enables the business strategy
3. **Strategy implementation**—Implementing business strategy enabled by the interaction between business and IT infrastructure and processes
4. **Technology implementation**—Interpreting the IT strategy via the requirements for IT infrastructure and processes

Figure 2 illustrates how the newer contexts of digital transformation can still be articulated in terms of combinations of the original four domains of the SAM. Given SAM’s sustained relevance, it is little wonder that it is still useful in articulating strategic alignment for digital transformation almost in defiance of its age.

### The Strategy Execution Gap

The strategy execution gap is the difference between the objectives articulated in an organization’s corporate strategy (the sum of business, IT, human...
resources (HR and operations strategies) and the results achieved from the execution of that strategy (figure 3). The gap could therefore originate in many different places within the organizational strategy (e.g., between any combination of the four SAM domains shown in figure 2).

The strategy execution gap is an enduring problem, with two-thirds of senior executives thinking that their organizations lack the right capabilities to execute their strategies, resulting in gaps between expectations and outcomes. This implies that the cause of the gap is in the “Business Strategy Implementation” and/or “IT Strategy Implementation” SAM domains.

The gap is such that organizations realize less than two-thirds of the financial performance their corporate strategy proposes and reflect that only 7 percent of staff members understand the expectations of them in executing the strategy. Furthermore, two-thirds of chief executive officers (CEOs) admit that they lack the capabilities required to create value, and 80 percent of executives admit that their strategy is not well understood in their organization. This version implies that the cause of the gap could be in any or all four SAM domains shown in figure 2.

These findings have major implications for governance. If the staff lacks strategic understanding in their roles, it is little wonder that the strategy execution gap is a concern. Some of the capability gap could be an outcome of poor alignment between IT and business and, thus, the poor allocation of organizational resources with respect to the organization’s strategy. Capability building, therefore, includes ensuring alignment between IT capabilities and corporate strategy execution.

Particularly challenging is that both IT and business alignment have a context in the complex environment within which the organization operates. In addition, factors such as technological evolution and changes in regulation, customer preferences, macroeconomy, and competition all impact organizational strategy and, thus, the nature of the required IT alignment.

**The Digital Strategy Execution Gap**

Two characteristics of strategic management are highlighted in SAM. These are strategic fit or the relationship between the external environment in which the organization competes, and the organization’s internal capabilities and functional integration or the relationship between business

---

**Figure 2—The 30-Year-Old SAM Domains Overlaid With Modern Digital Transformation Domains**

![Figure 2](image-url)
and IT capabilities. Thus, the IT strategy should be articulated both in terms of an external and internal domain,\textsuperscript{14} with a digital strategy being an element of the IT strategy. In this context, two key areas exist where an execution gap can occur:

1. Difficulties in translating the implications of the external environment on an organization’s competitiveness

2. Difficulties in the relationship between technology enablers and business execution

While point one previously is an enterprise governance challenge, point two highlights the area within which the digital strategy gap arises. The greater the difficulties in aligning IT with business, the greater the extent of unmet expectations and the greater the digital strategy gap.

The digital strategy execution gap is serious, with only 10 percent of enterprises from a sample of 340 large global enterprise senior executives having a plan to deploy their digital strategies,\textsuperscript{15} something akin to the finance gap in corporate strategy execution mentioned earlier.

Given that a digital strategy is an element of an enterprise strategy and that digital transformation is key to organizational resilience, sustainability and relevance, if only 10 percent is being executed, it is no surprise that less than two-thirds of the financial objectives expressed in the enterprise strategy are being missed. The survey responses from 1,591 senior business leaders in the United Kingdom and the United States termed the extent of the gap “a digital strategy execution crisis.”\textsuperscript{16}

Of those organizations that do implement digital strategies, only 38 percent of them being able to determine the outcomes of their digital transformation initiatives\textsuperscript{17} is a failure, not only to shareholders—an unknown return on investment (ROI) for the time, effort and money expended—but also to customers who will subsequently be attracted to competitors where the digital investments produce a rich, seamless and integrated customer experience. This speaks to the value and value propositions and financial outcomes of figure 1, again demonstrating poor alignment between the SAM domains these engage with shown in figure 2.

**Governance’s Role in Narrowing the Digital Strategy Execution Gap**

These issues should be better governed to reduce the severity and impact of the digital strategy execution gap. To minimize the strategy execution gap, governance professionals can:

- Ensure enterprise strategy efficacy, followed by IT (and digital) strategy efficacy, the latter of which may itself feed the enterprise strategy in a proactive paradigm. Possibly an implied
assumption of SAM, there is no point aligning poorly articulated strategies (SAM’s Business and IT strategy domains).

- Ensure an effective technology horizon scan to help determine the best enablers of corporate strategy objectives. A balance exists between considering proven technologies and new technologies that often offer little more than promises. Indeed, many challenges associated with the governance of innovation and innovative technologies exist. Selecting an inappropriate technology for the organization guarantees that part of a strategy will not be executed, thus facilitating a strategy gap (SAM’s IT Strategy domain).

- Note that IT may sometimes be in a stronger than expected position to propose new digital business models and, therefore, create new revenue streams. The overall governance challenge is to ensure consistency between analog and digital business models and manage the incremental risk of the digital innovation (SAM’s IT Strategy and Business Strategy).

- Distinguish between business as usual (BAU) operations and innovations that increase the organization’s relevance and sustainability, which is an important construct in digital transformation that will need appropriate oversight to ensure architectural fit and a valid allocation of resources, at least if the need to demonstrate ROI is required. This falls into an emerging field of governance called innovation governance.

- Ensure that organizational structures, governance (i.e., roles, responsibilities, accountabilities) and processes are realigned and monitored. Seventy-six percent of 80 senior executives from 20 countries and 25 industries cited employee interaction as a major constraint to strategy execution: “Executives know the barriers to long-term success are a lack of interaction and collaboration.” Furthermore, culture (behavior) has been recognized as one of the most significant critical success factors for successful IT implementation, with one-third of 2,135 global executives polled citing culture as the top barrier to digital transformation.

Boardroom Observations and Commentary

Because many root causes underly both strategy and digital strategy gaps, digital transformation presents great opportunity. However, many do not realize the anticipated benefits and, for some, a failed transformation challenges their very sustainability. Although digital transformation governance best practices are at low maturity, emerging boardroom practices, when applied smartly, can improve certainty of outcomes. Consider the four categories of practice highlighted in figure 4.

Talent and Expertise

Having the courage to recognize what is not known and ask for help may be an old adage, but it is fully applicable to digital strategy development and execution. Boards and management teams need to look in the mirror and critically assess whether they have the required talent and expertise to develop a digital strategy and to execute the transformation.

Because boards can be ill-prepared for digital transformation oversight, board skills need to be assessed and refreshed as needed. Steps to ensure competent execution include board education, advisors’ engagement and, if appropriate, the appointment of directors with the required expertise, all toward ensuring the competent execution of the directors’ fiduciary responsibilities. However, absent of a catalytic event, these take time to effectuate change.
Regulators are also increasingly critical of this level of board accountability. For example, in Canada, the Office of the Superintendent of Financial Institutions (OSFI) Corporate Governance Guideline (CGG) requires the board to approve and oversee the:

- Appointment, performance review and compensation of the CEO and other key members of senior management
- Mandate resources and budgets for the oversight functions

Indeed, board members are required annually to attest to their compliance under this guideline, ensuring that adequate and sufficient resources exist to execute the business plan and reduce the strategy and digital strategy gaps.

**Strategy Development**

As highlighted earlier, IT’s proactive role in strategy development is a rapidly developing paradigm. It is also a prerequisite in the development of any leading business strategy that is enabled by digital technology because these can only be developed through the fusion of great business and digital minds that fully understand digital capabilities and use cases to fully envision the strategic possibilities for the creation of new and innovative customer experiences, products, revenue streams and efficiencies.

Therefore, engaging proactive IT as equal partners in the strategy development and refresh processes is imperative. Doing so strengthens an organization’s ability to envision how markets evolve, shape the industry, and the manner in which it can lead and achieve its performance aspirations. However, a 2020 survey of 302 global c-suite executives in large organizations shows that IT develops an equal partnership with business only one-quarter of the time.

Specifically, an emerging board practice not only demands transparency in the enabling digital strategy but also targets customer experience.
outcomes, the enabling business model, operating model, supporting talent and workforce plans, which endorses SAM’s sustained relevance and the modern digital transformation domains articulated in figure 2.

Business Case and Resource Allocation
Enlightened boards are beginning to value digital transformation business cases that fully identify the opportunities and associated risk scale in a transformation execution plan that manages executive sponsorship, outcomes, performance metrics, project ownership and resource requirements.

Done well, this addresses the previously mentioned fact that two-thirds of CEOs and executives admit that they lack the capabilities to create value and execute their strategies.25, 26

Execution
To achieve target outcomes, boards include strategy and digital transformation reports that provide a keen lens on transformation oversight and execution, focusing on progress against key metrics, risk, opportunities and interventions to course correct where necessary at the quarterly board meetings.

“Transition risk management” is also gaining acceptance as a risk management framework that includes oversight of digital transformation risk, with the goal of achieving greater levels of certainty in the achievement of target outcomes. Transition risk defines the point where something defined as a risk begins to materialize.27 The top five transition risk factors include:28

1. Schedule delays
2. Service costs
3. High-demand skill sets
4. Service quality degradation
5. Managing service provider effectiveness

Moreover, boards also focus on ensuring that the right CEO and leadership team are in place, culture is evolving the way it needs to and employees are engaged in the strategy execution.

In terms of the right CEO and management team, digital transformation quite often requires different leadership skills, both during the transformation and operation of the business afterward. Boards have a duty to understand the new skills required and ensure that the right CEO and leadership team are in place to execute this digital transformation. The right CEO is not merely a permission giver, figurehead or an endorser; the right CEO is both the chief digital ambassador and arbiter of the digital vision, ensuring that the executive team remains committed to achieving the digital vision, thereby driving the elimination of the digital strategy gap.

Culture, too, needs to evolve as an important element of digital transformation. Examples include ensuring that leadership teams are instilling agility and the mentality that it is “OK to make mistakes, but learn from them and fail fast.” While every organization will face technological challenges in their digital transformation journey, “transforming an organization’s culture is more challenging.”30

Compared to Waterfall, Agile is a methodology better suited to achieving the desired agility because it deals with uncertain and unpredictable environments and helps ensure prioritization of the right (sub)projects.31 However, accommodating Agile and agility in a large organization steeped in a Waterfall culture is challenging.

Given the recruitment cost, talent war and poor employee engagement cost, the latter is high on many leaders’ agenda.32 Successful digital transformation
includes empowered employees who have the autonomy and tools they need to do their job successfully, leading to greater customer satisfaction, the ultimate outcome of digital transformation. To achieve this, boards are challenging management to ensure that through effective and continuous communications, each employee understands how the change impacts them, their roles going forward and ways they personally can contribute to the transformation and, eventually, enterprise performance in the new paradigm.

Done effectively, these strategies mitigate the previously mentioned facts that 80 percent of executives admit that their strategy is not understood in their organizations, only 7 percent of staff understand the expectations of them in executing the strategy, and organizations realize less than two-thirds of the financial performance their corporate strategy proposes.

These board trends are increasingly helping to better align IT with business to narrow the digital strategy gap.

Conclusion

The 30-year-old SAM continues to have the power to create an IT and overall digital transformation strategy that proactively contributes to an organization's digital future. The issue of a digital future has never been as important for so many businesses as it is today, if it is not already too late for them.

For those organizations that have implemented a digital strategy, many will have experienced a digital strategy gap, part of an enterprise strategy gap that ultimately results in a financial expectations gap for the organization. As an example, one part of a digital strategy under a particularly harsh spotlight under the coronavirus pandemic is BCP. It is now strongly in focus for organizations that, for example, found that their BCPs are not quite up to the task of a mass work-from-home requirement, in some cases resulting in financial losses for organizations due to lost business.

Ultimately, SAM showed itself to be one part of an important tool set that can help to narrow the digital strategy execution gap. The other part of the tool set is the evolution of governance demonstrated not only in theory, but also by means of the supporting enterprise governance trends found in today’s boardrooms.

Endnotes


7 Op cit Henderson and Venkatraman 1990


Go ahead and let me know if you need anything else! I'm here to help.
During the COVID-19 pandemic, many enterprises have stated that employee health and well-being are their primary concern. The events of 2020 have also led organizations to evaluate their preparedness for and responses to another major risk factor that they considered the most pressing issue just a few months ago: corporate governance.

A recent report encompassing a survey of more than 1,000 respondents examined the top risk concerns currently on the minds of global boards of directors (BoDs) and executives. The risk factors cited in this report cover a variety of topics: the economic climate, technology, human resources (HR), operations, competition and more.1

Despite their diversity, these risk factors share one thing in common: They all relate to corporate governance. Corporate governance encompasses the vision and mission of the enterprise and how the leadership seeks to accomplish that mission by establishing policies and procedures, setting ethical boundaries, delegating authority, ensuring quality and compliance, and meeting the needs and interests of its various stakeholders.

Sound corporate governance, of which sound IT governance is an integral part, can give boards and senior executives the power to ensure that their enterprises are effectively managing the risk conditions about which they are most concerned, in addition to those that are largely unforeseen. The numbers in the following headings reflect the ranking of each risk cited in the survey.

**Regulatory Change and Scrutiny of Operational Resilience, Products and Services (Number 1)**

During the COVID-19 crisis, organizations have been disrupted by the immediate need to change the way they do business at even the most fundamental levels, and IT has played an integral role. With offices and storefronts closed and vast numbers of employees suddenly transitioned to working from home, the operational resilience of functions such as cybersecurity, communications, transaction processing, auditing and many others has been put to the test. At the same time, organizations are asking their IT teams to think outside the box to leverage existing systems so they can continue to operate. In such an environment, sound IT governance is critical to accomplishing this outside-the-box thinking without exposing the organization to unacceptable levels of risk.

Although good governance is about much more than compliance and quality control, these are certainly fundamental aspects of it. A well-governed enterprise seeks to comply with all relevant laws, regulations and standards, and it has processes in place for doing so, but risk related to regulatory change is broader than a simple gap in compliance. Some regulatory changes have the potential to impact the value proposition of the whole

---

**Kevin M. Alvero, CISA, CFE**

Is senior vice president of internal audit, compliance and governance at Nielsen Company. He leads the internal quality audit program and industry compliance initiatives, spanning Nielsen’s global media products and services.
enterprise, and in an enterprise with sound governance, top leadership is scanning the horizon for regulatory changes that could be disruptive at the strategic level, including IT-related requirements involving privacy and cybersecurity.

Defining and ensuring the quality of products and services also fall under the purview of governance. The effective communication of expectations and a healthy culture, along with consistent and repeatable business processes (all governance-related concerns), can help ensure that products and customer experiences meet quality standards and support the enterprise's mission, values and value proposition.

Economic Conditions Impacting Growth (Number 2)

Changing economic conditions can affect, among other things, enterprises’ access to three key factors related to growth:

1. Credit
2. Investment funds
3. Markets

Organizations may not be able to control the volatility of the economy, but good governance—particularly the demonstration of good governance—can improve an organization’s position with regard to these three key factors.

In the late 1990s, organizations such as RepRisk and RobecoSAM began publishing environmental, sustainability and governance (ESG) ratings and, in 1999, the Dow Jones Sustainability Index became the first global index to track sustainability-driven public enterprises based on RobecoSAM’s ESG analysis. Today, most international and domestic public (and many private) enterprises are being evaluated based on their ESG performance by various third-party providers of reports and ratings.2 Not everyone fully accepts the utility of corporate governance rating systems. For example, some have expressed skepticism that any governance score based on a single set of value judgments about what constitutes good governance practices is a reliable measure of an enterprise’s governance. Indeed, the Society for Corporate Governance’s stated position is that “Many governance practice prescriptions tend to elevate form and appearance over substance.”3 Nevertheless, investment driven by ESG considerations remains high. According to a 2019 survey, 84 percent of investors agreed that corporations and business leaders should commit to balancing the needs of multiple stakeholders including shareholders, customers, employees, suppliers and local communities.4

Investors, lenders and gatekeepers who control access to markets are more likely to provide growth opportunities to enterprises they trust, and good governance is one way enterprises can earn that trust. Those responsible for IT governance should understand that the way an organization leverages technology has an impact on its perceived trustworthiness. According to a 2020 survey, trust in technology is down overall, and more than 60 percent of respondents agreed with the following statements:5

- The pace of change in technology is too fast.
- I worry technology will make it impossible to know if what people are seeing or hearing is real.

Government does not understand emerging technologies enough to regulate them effectively.

Succession Challenges and Ability to Attract and Retain Top Talent (Number 3)

Where there is an absence of good governance, there is an increased likelihood of fraud, bribery, corruption, waste, abuse, and unfair or unethical practices. Additionally, there may be a lack of clarity about the enterprise’s mission and values. These concerns contribute to unhappy employees, who, in turn, are harder to retain and less productive. In a well-governed environment, the opposite is true, making good governance essential to reduce the risk of being unable to hire the right people, keep them or maximize their potential.

Employees want to be well compensated, but they also want to understand the purpose and

“GOVERNMENT DOES NOT UNDERSTAND EMERGING TECHNOLOGIES ENOUGH TO REGULATE THEM EFFECTIVELY.”
significance of their work (and the organization’s mission) and the basis on which their success is evaluated. They also want fair access to opportunities for advancement, education and flexibility. For these reasons, sound governance makes an organization more attractive to employees who want to do good, grow and drive the success of their employer.

**Adoption of Digital Technologies That May Require New Skills (Number 10)**

It is imperative that business and IT leaders take a holistic view. When implementing new technologies, consideration should be given to how these technologies will enhance employee effectiveness and potential (and thereby job satisfaction), in addition to their inherent features and benefits. Top management should also cultivate a culture in which flexibility, comfort with change and continuous learning are the norm, as this will help current and future IT projects gain acceptance and demonstrate a satisfactory return on investment (ROI).

**Ability to Compete With “Born Digital” Enterprises (Number 4) and Resistance to Change (Number 5)**

One way governance is defined is “the act or process of providing oversight or authoritative direction or control.” Any significant change within an enterprise almost always requires strong top-down leadership. Without it, the most likely outcome is that nothing will change (maintaining the status quo), while everyone looks out for their own responsibilities and no one takes responsibility for the well-being of the whole. Opportunities will be missed, time and resources will be wasted, and change efforts will ultimately fail. Again, when leadership fosters a culture of continuous learning and comfort with change, it can avoid conflict with employee expectations.

On the surface, concern about “born digital” competitors may seem to be driven by external pressure from newcomers entering the market, and it is. But it has just as much to do with an organization’s ability to manage its own digital transformations. A successful digital transformation requires a strategic, coordinated effort. Permitting digital transformation to be managed by the various business areas based on their own needs results in efforts that are divergent, redundant and/or contradictory. The board, senior management and IT leadership have the power to ensure that people with the right skills and expertise are tasked with implementing new technologies and processes with the proper authority, support and funding to succeed.

**Cyberthreats (Number 6) and Privacy and Identity Management and Information Security (Number 7)**

Information security was identified in two of the top 10 places in the survey, reflecting enterprises’ current reality. On the one hand, they must protect the data and information in their possession from malicious parties who seek unauthorized access to it for their own gain. On the other hand, consumers are demanding greater control and transparency with regard to how enterprises use their data for legitimate business purposes and the risk to which this exposes consumers. Technology solutions are an integral part of managing data privacy and security concerns, but most enterprises understand that these are not solely technology issues. The key to managing risk lies in sound governance over both data and IT. Governance establishes the enterprise’s mission and its commitment to its stakeholders. It also establishes who is responsible and accountable for data privacy and security, what policies and procedures are in place to guide the enterprise’s actions, and what types of controls and reporting mechanisms have been implemented to ensure quality, security and compliance.

**Organizational Culture Does Not Encourage Timely Identification and Escalation of Risk Issues (Number 8)**

IT can play a critical role in ensuring that risk factors are identified and escalated in a timely manner. For example, organizations can use artificial intelligence (AI) to scan social media for potential reputational risk or to monitor supply chains for potential disruptions and failure points. They can leverage automation to perform continuous auditing processes, sampling large populations of data to detect irregularities and quickly escalating issues that require human intervention. These capabilities are most powerful when deployed in a well-governed environment to enhance human
stewardship. That is why it is critical that top management foster a culture that supports the timely reporting of risk issues. Regardless of the systems put into place to detect risk, if the culture is such that employees believe it is best to remain silent and follow orders, then technology-enabled detection and escalation systems will be less effective, and top leaders can be virtually certain they are receiving incomplete information with regard to risk factors affecting the enterprise.

Customer Loyalty and Retention (Number 9)

It should be intuitive that commitment to customer loyalty drives profitability, and research provides evidence that this is so. Nevertheless, incentive structures and a focus on short-term performance can sometimes motivate employees to make decisions that destroy customer value and loyalty rather than build it up. If board members and senior leaders want to mitigate risk related to customer loyalty and retention, they must empower their employees to do whatever is needed to satisfy (or even delight) customers and reward them for doing so. The organizations that do this best (the “loyalty leaders”) grow revenue roughly 2.5 times faster than their industry peers. As more and more interaction between organizations and their customers becomes technology-enabled, greater responsibility for the end-to-end customer experience will fall under the purview of IT governance.

Conclusion

While striving to adapt to the continuously evolving landscape of top-level risk factors, leaders can understandably become focused on tactical solutions and short-term objectives, which are necessary. But it is important to bear in mind that good corporate governance—and, as a microcosm, good IT governance—acts as the compass that directs the enterprise’s perception of, and response to, risk—whatever that risk may be.

Endnotes


3 Society for Corporate Governance, “Statement on Governance,” https://www.societycorpgov.org/about76/statementongovernance


9 Ibid.
Concerns about privacy risk have triggered a number of new privacy protection regulations: The US State of California Consumer Privacy Act (CCPA) went into effect on 1 January 2020, the Brazilian General Data Protection Law (LGPD) becomes effective in August 2020, China has completed the first draft of a personal information protection law, New Zealand's privacy law is likely to take effect in mid-2020, and the EU General Data Protection Regulation (GDPR) will be replaced as an applicable law in the United Kingdom at the end of 2020. The increasing trend of privacy legislation exacerbates privacy risk, which is a trigger for privacy protection requirements and influences consumer trust and enterprise reputation. So, what is privacy risk? From what is privacy risk arising?

What Is Privacy Risk?
Privacy risk is the likelihood that individuals will experience problems resulting from data processing, and the impact of these problems should they occur. Privacy risk includes but is not limited to technical measures that lack appropriate safeguards, social media attacks, mobile malware, third-party access, negligence resulting from improper configuration, outdated security software, social engineering and lack of encryption.

According to article 4 of GDPR, data processing is a set of operations including but not limited to the collection, storage, adaptation or alteration, disclosure by transmission, and dissemination of data. ISACA® provides a data life cycle model that can be taken into consideration when building a data inventory (figure 1).

Privacy risk can exist throughout the data life cycle, so it is important to manage and govern data properly. A number of privacy risk management activities can be undertaken during the data life cycle. Designing a privacy risk management framework is the first step to ensure data validation and data protection, to monitor and control data, and to comply with all applicable laws and regulations.

Creating and Implementing a Privacy Risk Management Framework
The globally recognized COBIT® 2019 framework can serve as a foundation to ensure effective enterprise governance of information and technology (EGIT). It can help an enterprise govern data, implement internal and external security, and determine the components needed from other frameworks. It is a useful tool for implementing a privacy risk management framework, particularly by focusing on the four management domains (figure 2):

1. Align, Plan and Organize (APO)
2. Build, Acquire and Implement (BAI)
3. Deliver, Service and Support (DSS)
4. Monitor, Evaluate and Assess (MEA)
**Figure 1—Data Life Cycle Mapping With Data Inventory Considerations**

<table>
<thead>
<tr>
<th>PLAN/DESIGN</th>
<th>BUILD/ACQUIRE</th>
<th>STORE</th>
<th>USE</th>
<th>SHARE</th>
<th>ARCHIVE/DESTROY</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the context and purpose of the repository?</td>
<td>Where are the data moving from and to?</td>
<td>What kind of information is in the repository?</td>
<td>How is the information being used?</td>
<td>Where will the data flow (from country to country)?</td>
<td>What data are currently being retained, how and where?</td>
</tr>
<tr>
<td>Who is the owner of the repository?</td>
<td>How much data are in the repository?</td>
<td>In which country or countries are the data stored?</td>
<td>From which country or countries is the data accessed?</td>
<td>Are the data shared with third parties? Are they controllers, joint controllers or processors?</td>
<td>What are the scenarios that would require data retention or destroy?</td>
</tr>
<tr>
<td>Is the data dictionary design compatible with different systems?</td>
<td>Is this a paper or electronic repository?</td>
<td>Are there any technical safeguard measures for data storage?</td>
<td>Are the data applied to automated decision making?</td>
<td>Is the data sharing obtained with explicit consent from data subjects?</td>
<td>Do the technical measures taken for data destruction guarantee they are irrecoverable?</td>
</tr>
<tr>
<td>Is the data dictionary design compliant with laws and regulations?</td>
<td>Are the data structured or unstructured?</td>
<td>Are the data stored in the cloud?</td>
<td>Is there any legal basis provided for the data usage?</td>
<td>Is there any DPIA conducted for data sharing?</td>
<td>Are the data archived/destroyed in compliance with laws and regulations?</td>
</tr>
</tbody>
</table>

**Figure 2—Mapping to COBIT®**

<table>
<thead>
<tr>
<th>Privacy Risk Management Framework</th>
<th>COBIT® 2019</th>
</tr>
</thead>
</table>
| Stage 1: Establish privacy governance | BAI01 Managed programs  
BAI11 Managed projects |
| Stage 1-1: Define privacy governance goals | APO01 Managed information and technology (I&T) management framework  
APO02 Managed strategy  
APO03 Managed enterprise architecture |
| Stage 1-2: Establish enterprise privacy risk management framework | APO04 Managed innovation  
APO05 Managed portfolio |
| Stage 1-3: Realize the benefits of privacy risk management | APO06 Managed budget and costs  
APO07 Managed human resources  
APO08 Managed relationships |
| Stage 2: Conduct privacy risk management activities  
Stage 2-1: Define privacy risk assessment framework | APO12 Managed risk |
| Stage 2-2: Conduct privacy risk assessments  
Stage 2-2-1: Vendor/third-party risk assessments  
Stage 2-2-2: Data breach readiness assessments | APO09 Managed service agreements  
APO10 Managed vendors  
DSS02 Managed service requests and incidents |
| Stage 3: Implement risk response  
Stage 3-1: Establish response procedures for privacy risk | DSS03 Managed problems |
| Stage 3-2: Response to privacy risk | DSS04 Managed continuity |
| Stage 3-3: Evaluate privacy risk response | MEA01 Managed performance and conformance monitoring  
MEA02 Managed system of internal control  
MEA03 Managed compliance with external requirements  
MEA04 Managed assurance |
Stage 1: Establish Privacy Governance
The US National Institute of Standards and Technology’s (NIST) Privacy Framework is intended to assist organizations in communicating and organizing privacy risk and rationalizing privacy to build or evaluate a privacy governance program. The NIST Privacy Framework defines privacy governance as govern/develop and implement the organizational governance structure to enable an ongoing understanding of the organization’s risk management priorities that are informed by privacy risk. In this stage, the enterprise could do the tasks outlined in figure 3.

Stage 1-1: Define Privacy Governance Goals
The first step is for the enterprise to create a privacy vision and mission statement. Stakeholders should take market expectations into consideration, establish an overall privacy risk management strategy, define the scope of privacy governance by identifying applicable personal data protection laws and regulations, structure a privacy team, and define a privacy risk tolerance level.

Specific and clear communication about the enterprise’s approach is key to obtaining support for the privacy risk management program. But it should be noted that there is no one-size-fits-all strategy. The enterprise must consider its own circumstances and the business environment when adopting a privacy strategy.

Stage 2: Conduct Privacy Risk Management Activities
NIST also states that a privacy risk management framework is intended to help enterprises weigh the benefits of data processing against the risk of doing so and determine which risk response measures should be adopted. In this stage, enterprises could conduct the tasks listed in figure 4.

Stage 1-2: Establish Enterprise Privacy Risk Management Framework
An enterprise privacy risk management framework consists of the following elements:

- **Purpose**—Explain privacy governance goals in detail.
- **Scope**—Define the personal data required to be protected and the internal policies to be followed.
- **Risk**—Identify potential risk factors, vulnerabilities and threats related to data processing activities.
- **Responsibilities**—Set up a privacy committee consisting of identified stakeholders, specify the role of each department (e.g., which executives must approve funding for the privacy team), establish the role of the data protection officer, support privacy initiatives such as training and awareness, and hold employees accountable for following all privacy policies and procedures.
- **Processes**—Establish privacy risk management processes.

Stage 1-3: Realize the Benefits of Privacy Risk Management
A privacy risk management framework is intended to help enterprises weigh the benefits of data processing against the risk of doing so and determine which risk response measures should be adopted.

**Figure 3—Creating and Implementing a Privacy Risk Management Framework—Stage 1: Establish Privacy Governance**

<table>
<thead>
<tr>
<th>Stage 1-1</th>
<th>Stage 1-2</th>
<th>Stage 1-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define privacy governance goals</td>
<td>Establish enterprise privacy risk management framework</td>
<td>Realize the benefits of privacy risk management</td>
</tr>
</tbody>
</table>
Stage 2-1: Define Privacy Risk Assessment Framework

A privacy risk assessment determines whether an enterprise is in compliance with applicable laws and regulations, industry standards, and internal policies and procedures. Based on a survey by the International Association of Privacy Professionals (IAPP) and TrustArc, the vendor/third-party risk assessment is the most common type of assessment conducted (figures 5 and 6). Also common are data protection impact assessments (DPIAs), privacy impact assessments (PIAs) and legitimate interest assessments (LIAs).

A DPIA is designed to identify risk arising from the processing of personal data and to minimize this risk as much and as early as possible. DPIAs can help prioritize risk, allowing resources to be concentrated on the domain with the highest risk and the greatest potential damage in order to mitigate that risk.

A PIA is an analysis of the risk factors associated with processing personal information in relation to a project, product or service. PIAs provide remediation measures to avoid or mitigate risk. In addition to COBIT 2019, several others are available to help enterprises address privacy risk:

- **NIST Privacy Framework**—Version 1.0 of the NIST Privacy Framework, released in January 2020, is a tool to assess and mitigate privacy risk, implement privacy engineering, and design products and services to protect individuals’ privacy by providing a set of activities and outcomes that enables enterprise stakeholders to discuss managing privacy risk (figure 7).

- **International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 27701**—This first global privacy standard, released in August 2019, provides a risk-based framework for a privacy risk management system. It helps enterprises translate principles-based legal requirements into technical privacy controls that can be implemented in tandem with security controls (figure 8).
Figure 7—Mapping to NIST Privacy Framework

<table>
<thead>
<tr>
<th>Privacy Risk Management Framework</th>
<th>NIST Privacy Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage 1: Establish privacy governance</td>
<td>Governance policies, processes and procedures (GV.PO-P)</td>
</tr>
<tr>
<td>Stage 1-1: Define privacy governance goals</td>
<td>Governance policies, processes and procedures (GV.PO-P)</td>
</tr>
<tr>
<td>Stage 1-2: Establish enterprise privacy risk management framework</td>
<td>Business environment (ID.BE-P)</td>
</tr>
<tr>
<td>Stage 1-3: Realize the benefits of privacy risk management</td>
<td>Business environment (ID.BE-P)</td>
</tr>
<tr>
<td></td>
<td>Data protection policies, processes and procedures (PR.PO-P7, PR.PO-P8)</td>
</tr>
<tr>
<td>Stage 2: Conduct privacy risk management activities</td>
<td>Risk management strategy (GV.RM-P)</td>
</tr>
<tr>
<td>Stage 2-1: Define privacy risk assessment framework</td>
<td>Risk assessment (ID.RA-P)</td>
</tr>
<tr>
<td>Stage 2-2: Conduct privacy risk assessments</td>
<td>Data protection ecosystem risk management (ID.DE-P)</td>
</tr>
<tr>
<td>Stage 2-2-1: Vendor/third-party risk assessments</td>
<td>Data protection policies, processes and procedures (PR.PO-P7, PR.PO-P8)</td>
</tr>
<tr>
<td>Stage 2-2-2: Data breach readiness assessments</td>
<td>Data protection policies, processes and procedures (PR.PO-P10)</td>
</tr>
<tr>
<td>Stage 3: Implement risk response</td>
<td>Data protection policies, processes and procedures (PR.PO-P7)</td>
</tr>
<tr>
<td>Stage 3-1: Establish response procedures for privacy risk</td>
<td>Monitoring and review (GV.MT-P)</td>
</tr>
<tr>
<td>Stage 3-2: Response to privacy risk</td>
<td>Data protection policies, processes and procedures (PR.PO-P7)</td>
</tr>
<tr>
<td>Stage 3-3: Evaluate privacy risk response</td>
<td>Monitoring and review (GV.MT-P)</td>
</tr>
</tbody>
</table>

Source: Adapted from International Association of Privacy Professionals (IAPP) and TrustArc, Measuring Privacy Operations 2019: Cookies, Local vs. Global Compliance, DSARs and More, USA, 2019
Stage 2-2: Conduct Privacy Risk Assessments
A privacy risk assessment is one of the critical procedures in privacy risk management. The aim is to assist enterprises in identifying the possible risk, vulnerabilities and threats during the data life cycle. There are many types of privacy risk assessments, which include vendor/third-party risk assessments and data breach readiness assessments (figures 5 and 6).

Stage 2-2-1: Vendor/Third-Party Risk Assessments
According to the IAPP survey, the most common type of risk assessment (performed by 63 percent of respondents, as shown in figures 5 and 6) is the vendor/third-party risk assessment.15 The greater an enterprise’s dependence on third parties or nth parties, the more complex a third-party risk assessment must be. Enterprises should consider the following factors related to threat, vulnerability and maturity:

- Determine whether the third party is aware of the core requirements of data protection.
- Check whether a DPIA has been conducted for the data processing operations performed by the third party; conduct a request for information (RFI)/request for quotation (RFQ), an on-site check, and regular audit and monitoring of the usage of software development kits (SDKs).

Stage 2-2-2: Data Breach Readiness Assessments
According to the IAPP survey, the most common type of risk assessment (performed by 63 percent of respondents, as shown in figures 5 and 6) is the vendor/third-party risk assessment.15 The greater an enterprise’s dependence on third parties or nth parties, the more complex a third-party risk assessment must be. Enterprises should consider the following factors related to threat, vulnerability and maturity:

- Determine whether the third party is aware of the core requirements of data protection.
- Check whether a DPIA has been conducted for the data processing operations performed by the third party; conduct a request for information (RFI)/request for quotation (RFQ), an on-site check, and regular audit and monitoring of the usage of software development kits (SDKs).
• Review whether the third party has certifications such as ISO/IEC 27001, Payment Card Industry Data Security Standard (PCI DSS) or other information security-related certifications.

• Review data sources, data types, data location, local regulatory requirements, data retention period, minimum safeguards and additional processing purposes, such as subcontracts to fourth or fifth parties.

• Review potential data combinations and additional uses that may impact the level of risk for individuals (e.g., artificial intelligence [AI], machine learning [ML], cloud computing technology) and whether the third-party possesses relevant qualifications.

• Disclose to customers any use of subcontractors to process personally identifiable information (PII).

• Cooperate only with third parties who can prove their compliance and provide adequate safeguards.

• In the case of general written authorization, inform customers of any intended changes concerning the addition or replacement of subcontractors.

**Stage 2-2-2: Data Breach Readiness Assessments**

To prepare for a data breach, assess the following:

- Level of risk of a data breach:
  - Considering the nature, scope, context and processing purpose of an incident, evaluate the risk associated with an independent event. If it affects large-scale data subjects or has a greater impact on specific individuals, the risk is high.

- Likelihood and severity of a personal data breach:
  - Type and nature of personal data involved, particularly special categories of personal data
  - Circumstances of a personal data breach
  - Whether appropriate technical safeguards have been applied (e.g., encryption, pseudonymization)
  - Whether the data subject will be directly or indirectly affected
  - Possibility that pseudonymization can be restored or that confidentiality fails
  - Possibility that personal data can be maliciously used
  - Possibility of substantial damage on a physical level
  - Nonsubstantial damage to the data subject

Several entities provide methodologies for data breach readiness assessments, including the following:
European Union Agency for Cybersecurity (ENISA)—ENISA’s methodology for assessing the severity of personal data breaches can be applied to identify and mitigate risk.\(^{16}\) The criteria used to analyze the severity of the breach (SE) are data processing context (DPC), ease of identification (EI) and circumstances of the breach (CB), plus other factors that influence the overall scale of the breach: \(SE = DPC \times EI + CB\)

Spanish Data Protection Agency—The Agencia Española Protección Datos (AEPD) has established a set of criteria to assess risk based on the following factors: category or critical level; nature, sensitivity and categories of personal data affected; legible/illegible data; volume of personal data; ease of identifying individuals; severity of the consequences for individuals; individuals with special characteristics; number of individuals affected; data controllers with special characteristics (the entity itself); profile of the user affected; number and classification of the systems affected; impact; and legal and regulatory requirements.\(^{17}\)

Stage 3: Implement Risk Response
Implementing the privacy risk response is the last stage of implementing a privacy risk management framework. In this phase the enterprise shall establish response procedures for privacy risk, take appropriate responses to the identified privacy risk and evaluate the privacy risk response. In this stage, the enterprise could do the tasks listed in figure 10.

Stage 1: Establish Response Procedures for Privacy Risk
After identifying privacy risk factors, enterprises should establish risk response procedures, taking into consideration the following aspects:

- Privacy policy
- Information security architecture
- Human resources (HR) controls
- Asset management

Stage 2: Response to Privacy Risk
After identifying privacy risk, enterprises should take the appropriate action:

- **Mitigate risk**—Adopt the appropriate technical or administrative approaches in systems, products or services to minimize risk until an acceptable risk tolerance level is reached. Technical approaches include obfuscation technology, data minimization technology, security technology and privacy engineering technology. New technologies on the horizon include zero knowledge proofs, homomorphic encryption, secure multiparty computation, differential privacy, edge computing and local processing, device-level machine learning, identity management, small data, synthetic data sets, and generative adversarial networks.\(^{18}\)
- **Transfer risk**—Sign contracts with the other enterprises involved.
- **Share risk**—Implement privacy notice and consent mechanisms as a means of sharing risk with individuals.

Stage 3: Evaluate Privacy Risk Response
Evaluation of the enterprise’s privacy risk response should be ongoing to control, manage and report risk related to privacy risk management practices.
At the same time, the enterprise should designate a specific person who is responsible for monitoring the privacy risk response, based on the enterprise’s privacy risk governance goal. Monitoring ensures that implementation of the privacy plan is consistent with the enterprise’s current privacy policies and standards. In addition, evaluation of the privacy risk response ensures achievement of the enterprise’s privacy purpose by detecting failures early and obtaining feedback for improvement. When enterprises evaluate their privacy risk response, they should consider three indicators:

- **Compliance**—Can the enterprise ensure necessary policies and controls are in place for compliance during the collection, use and retention of personal data?
- **Regulation**—Does the response meet the requirements of applicable laws and regulations, which are constantly changing?
- **Environment**—Is there a risk of physical harm, programmatic concerns or insider threats?

In particular, enterprises should carry out incident response reviews or post-incident evaluations after a security incident occurs. This includes reviewing configurations of personnel and resources and evaluating control approaches such as time and procedures.

**Privacy Risk Management in Practice**

Two real-life examples are provided here. The first focuses on performing a qualitative risk assessment based on an existing methodology. The second deals with one of the hottest privacy issues—employee tracking and monitoring—and how to implement privacy risk management in this scenario.

**Example 1: Data Breach Risk Assessment Using the ENISA Methodology**

In this example, two types of HR-related data breaches have occurred:

- **Case 1**—A file available on a shared drive containing more than 500 employees’ names and dates of birth is accessed by nonauthorized employees.
- **Case 2**—An external contractor mails the monthly pay slips of eight employees to unauthorized recipients.

By applying the ENISA model, the severity of the personal data breaches can be assessed.

For the first case:

- **DPC**—The names and dates of birth are simple data, so DPC = 1.
- **EI**—Because both the full name and the date of birth may be disclosed to others, there are two identifiers that can single out the individual, so EI = 1 (maximum).
- **CB**—The circumstance is loss of confidentiality. Nonauthorized employees can access the data, which means that the data can be disclosed to a number of known recipients, so CB = +0.25.

Therefore, SE = 1x1 + 0.25 = 1.25.

For the second case:

- **DPC**—The information on the pay slips is financial data, in particular, the kind of data that comes from a bank and concerns the account balances of clients for the last month, so DPC = 3.
- **EI**—The combination of information on the pay slips, such as full name and Social Security number, makes it easy to identify the individual, so EI = 1 (maximum).
- **CB**—Although the circumstance is the same as in the first case, the personal data have been sent to unauthorized recipients, which increases the impact of the breach because of the unknown number of recipients, so CB = +0.5 (higher than in the first case).

Therefore, SE = 3x1 + 0.5 = 3.5.

By conducting this type of qualitative assessment, an enterprise can evaluate the severity of breaches,
which can help it prioritize its resources and influence privacy-related decision making.

Example 2: Employee Tracking and Monitoring
Few data controllers are likely to collect more personal data about individuals than their employers. So employee tracking and monitoring tools, such as those listed here, can impose a high privacy risk in the workplace:

- **Bring your own device (BYOD)**—Employees are permitted to use their own personal devices (e.g., smartphones, tablets) for communicating in the workplace. This results in a data protection risk because, outside the workplace, employees’ mobile devices might be lost or misused; inside the workplace, the employer has access to personal data from employees’ personal devices.

- **Data loss prevention (DLP)**—DLP tools inevitably involve processing the personal data of employees and other third parties because they operate on networks and systems used by employees, such as the email exchange server, which can contain personal information even if employees are not allowed to use it for personal activities.

- **Closed-circuit television (CCTV)**—CCTV is used to monitor the workplace for security purposes.

- **Email monitoring**—During an internal investigation, the employer may review employees’ emails.

- **Global Positioning System (GPS) tracking**—GPS tracking devices may be installed in company cars.

Stage 1: Establish Privacy Governance
Before deciding whether to apply these monitoring tools, the enterprise should judge whether their use is based on data subject consent or legitimate interests. At the same time, the enterprise should establish appropriate policies (such as BYOD policies) and clearly explain to employees the purpose of collecting their personal data and the enterprise's responsibilities when doing so. For example, when deciding to apply DLP tools, the enterprise should strengthen the protection of its IT infrastructure and confidential business information through internal and external strategies.

Stage 2: Conduct Privacy Risk Management Activities
The enterprise should carry out a DPIA, LIA or balancing test on the employee monitoring activities to determine necessity, legitimacy, proportionality and transparency.

- **Necessity**—Whether monitoring is necessary to the processing purpose and meets data minimization requirements

- **Legitimacy**—Whether monitoring (e.g., large-scale video surveillance or the systematic monitoring of public areas) meets legitimate interests, such as protecting the IT infrastructure of maintaining the safety of public areas

- **Proportionality**—Whether monitoring is proportionate to the issue the enterprise is encountering (e.g., remote control, facial recognition and voice recording may not be necessary)

- **Transparency**—Whether the existence and type of surveillance measures have been communicated to employees

Stage 3: Implement Risk Response
Be clear about where the processed data are stored and what measures must be taken to keep them secure.

- Ensure that the transfer of data from employees’ personal devices to the enterprise’s servers is secure to avoid any interceptions.

- Consider how to manage personal data held on personal devices once an employee leaves the company or if a device is stolen or lost. Mobile device management software can be used to locate devices and remove data on demand.

- Obtain prior authorization when required. For instance, in most countries, enterprises installing CCTV should obtain advance certification from supervisory authorities, in accordance with local regulations.

- After monitoring has been implemented, make the following determinations with regard to personal data: whether there is a legal basis for retaining data; whether the data are stored safely; whether the data retention period is defined; whether data subjects can exercise their rights, including the right to complain; whether the data will be anonymously processed or destroyed.
Conclusions
Privacy is not just a compliance issue anymore. It is about managing consumer trust and safeguarding personal data during the data life cycle. Creating and implementing a privacy risk management framework is the critical step an enterprise should take to build trust and protect data.

"PRIVACY...IS ABOUT MANAGING CONSUMER TRUST AND SAFEGUARDING PERSONAL DATA DURING THE DATA LIFE CYCLE."

Endnotes
3 Intersoft Consulting, Art. 4: Definition, EU General Data Protection Regulation (GDPR), Belgium, 2018, https://gdpr-info.eu/art-4-gdpr/
6 ISACA, COBIT® 2019, USA, 2018, https://www.isaca.org/resources/cobit
8 Ibid.
11 Ibid.
12 Op cit National Institute of Standards and Technology
19 Op cit ENISA
Mercury NZ, a US$2 billion renewable energy generation and retail company, has the most NZ Stock Exchange shareholders of any New Zealand company, serving more than 373,000 residential, commercial, industrial and spot customers across New Zealand. The company employs 775 full-time employees (FTEs) plus an additional approximately 700 contractors. Founded in 1999, Mercury NZ has grown organically over the last 21 years and has transitioned over time to adopt increased use of connected technologies. As an energy producer and retailer, Mercury NZ manages operational technology (OT) and information technology (IT) infrastructures and networks.

As the business has evolved and new connected technologies have been deployed, structured security at Mercury NZ, as with many growing organizations, was introduced post-operationalization of many systems, delivering services to both internal and external customers and other stakeholders.

The Challenge

Mercury NZ is an innovative technology-driven business. The business realized that to be able to take full advantage of technology, it must optimize technology-related business risk and, in 2018, began the journey to mature its security management capabilities.

Like many similar organizations, security activities were decentralized and dotted across the organization and lacked formal rigor and formal capability maturity assurance processes. Anecdotally, capability maturity was relatively low, and the business was not optimizing the value of security controls through new business technology solutions. New technologies were often implemented at pace but without the necessary formal security rigor. Therefore, Mercury NZ took the initiative to centralize security management and formalize security rigor around its technology innovations and general security operations to uplift security capability maturity across the organization.

The Mercury NZ executive team realized that the establishment of an effective enterprise security management function was fundamental to the business’s ability to maintain the trust and confidence of its stakeholders—both internal and external.

The Solution

By June 2018, Gabriel T. Akindeju, a seasoned security industry professional, joined the employ of Mercury NZ as its first enterprise security manager.1 Akindeju’s charge was to annex, leverage and reorient various security activities within the business and build a strategic program that would enhance protection of the organization’s infrastructure and data and instill a security culture. This had to be accomplished despite the challenges

Katie Teitler

Is a senior analyst at TAG Cyber, where she collaborates with security product companies on market messaging, positioning and strategy. In previous roles, she has managed, written and published content for two research firms, a cybersecurity events company and a security software vendor. Teitler is a co-author of Zero Trust Security for Dummies.
of a highly distributed workforce (corporate office workers, field workers and contractors), two distinct business units (generation and retail), separate technology environments and limited history of security awareness.

Akindeju instantly realized that building a security and risk program that would suit the company’s needs required more than a single-person effort. For the program to achieve success, he would need to engage company leadership and enlist organizationwide champions.

Listen, Learn, Educate, Recommend

On his first day at Mercury NZ, Akindeju reached out to colleagues to schedule coffee sessions and informal meetings. Understanding that executives’ time is valuable, Akindeju stuck to a strict policy of scheduling no more than 15–30 minutes with each individual, and the agenda for each meeting was not security—it was to meet people, introduce himself, and listen to business leaders’ goals and objectives for their area of responsibility.

"Understanding what is important to people, how they work, how their teams work, what their priorities are—these are factors that need to be built into a security and risk program. Technology had already been brought in to enable the business—to make things work better, to be more efficient—so security could not stand in the way of that progress. I knew I needed to enable productivity but do so in a secure way and in a way that would instill confidence," Akindeju said.

Though the purist security-centric approach to some of Mercury’s technology concerns might have been to make major adjustments right away, Akindeju decided that forming relationships and recruiting business partners would serve the company—and his eventual team—better in the long term. He understood that the business’s primary responsibilities were to customers and other stakeholders and that any security deliverables must support the company’s purpose “to inspire New Zealanders to enjoy energy in more wonderful ways.”

Akindeju learned that Mercury’s employees were friendly and willing to help. This was a positive attribute for company culture and workplace satisfaction, but as a security practitioner, Akindeju knew that these inclinations also created a vulnerability, namely, social engineering. Considering that social engineering (phishing and stolen credentials, in particular) is often the initial vector in a cyberattack, Akindeju decided that the first official security activity would be to scope the extent of the problem.

Akindeju hired external consultants to conduct penetration tests focused specifically on socially engineering Mercury’s employees. Immediately following, when the exercise was fresh in people’s minds, Akindeju presented the findings to executives and used the findings to demonstrate what had happened and explain why and how (in a real-life situation) particular employee behaviors put the business at increased risk for a cyber incident.

“It was important,” Akindeju said, “to bring home the message that the social engineering threat is real, that it is not something we only see on TV or movies; it is something that can happen here, and it can negatively impact our business.”

After he had fully explained the business risk, Akindeju worked with the company’s People and Performance (i.e., human resources [HR]) team and recommended new policies and practices the organization could use to reduce the likelihood of a successful social engineering attack. Some of the recommendations included:

- Implementation of a staff identification (ID) and physical access policy
- A security awareness training program to include theater-style presentations, video skits, guidance on how to comply with the policy and instructions for what to do if noncompliance was observed
- New systems access processes to enforce technical system controls

By establishing a direct link between action and risk, Akindeju was able to gain support and approval for his program and affect a positive security outcome for the security program.
Simplicity and Clarity

His next action item was to develop a more robust security and risk management plan that he could present to Mercury’s leadership team. While the concept of “robust” implies “exhaustive,” Akindeju committed himself to creating a one-page plan that was easy for nonsecurity people to understand. “If there is one thing I have learned over the course of my career,” he said, “it is that if you make things too complex, people will not be able to follow. If they cannot follow, they will not buy in to your ideas.” Because his responsibility was to gain support for a new program, he needed to be clear, concise and straightforward.

To ensure simplicity for a complex problem, Akindeju drew on established industry frameworks including COBIT®, the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 27001-2/5 and the International Society for Automation (ISA) standard ISA/IEC 62443 to map the current state and the potential path to the desired target state. Once he could see the company’s security posture laid out on paper, it was easier to identify areas of greatest concern. For instance, Akindeju observed that the rate of change in the technology environment at Mercury was high, but solutions were not always formally assessed for security. Also, although anecdotal practices suggested some controls were put in place, they were not optimized for value.

Fortunately, Akindeju also recognized that this was a learned behavior, not malicious or stubborn behavior. Employees wanted to deliver technology to improve internal and external operations, but they had never received effective training on how to include security or compliance in their processes. Thus, Akindeju began speaking with architects about how to properly design security and avoid compliance issues. He again relied on COBIT, ISO 27001-2/5 and ISA/IEC 62443 to map risk, demonstrate gaps and explain the consequences of risky decisions to his colleagues, and he provided actionable recommendations they could employ going forward (figure 1).

Education became Akindeju’s tool for influence and he found Mercury employees willing to learn. He focused on the value of technology to the organization—something that was already established when he joined the company—and explained how a malware infection, for instance, could render tools, systems and data unavailable. Without access to or availability of those assets, those tools’ and systems’ value would be significantly diminished and could negate the “Energy Freedom” mission of the company. As a mission-driven organization, the message of deprecated value resonated.

Recruit, Train, Execute

An integral part of Akindeju’s plan was the tried and true method of identifying and recruiting security champions from different functional units within the company. As a new security practice, he knew he needed support. He focused on finding individuals who influenced the way their departments functioned. These did not have to be people with management titles, but they had to be leaders who

<table>
<thead>
<tr>
<th>Figure 1—Actionable Security Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Problem</strong></td>
</tr>
<tr>
<td>Lack of formal consideration for security during design</td>
</tr>
<tr>
<td>Lack of formal consideration for security through delivery</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
among peers. Because he did not want security to be perceived as a hammer, Akindeju decided to ask employees for nominations for his task force, the Security Chapter. In parallel, he wrote his own private list of individuals he thought might make good champions; not so coincidentally, the nominations and Akindeju’s list overlapped. Though the goal of the exercise was to identify potential champions, Akindeju had grander plans. With the support of upper management, he organized three days of security fundamentals training for all technology employees and provided an extra two days for the individuals nominated by peers. The latter group, totaling 25 employees from marketing, IT, service management and more, sat for a certification exam, received certificates and became an extended security team of sorts that helped push the security message throughout the organization (figure 2). This team helped ensure that security was part of the conversation for new technology and process deployments across the entire business.

As Akindeju did not yet have a fully-fledged security team, his workload increased significantly. He developed and presented a business case for an elastic co-sourcing arrangement that would allow him to hire external security consultants who could help drive secure-by-design principles, review new and existing deployments, handle exemptions based on risk, identify and remediate security gaps (when possible) with existing tools, and ensure that delivery processes met the principles of the security
Akindeju plugged into existing technology governance functions and also established enterprise-level technology risk and security governance over technology procurement to avoid shadow IT and insecure implementation, and for healthy discussions on return on investment (ROI) on security investments.

The Benefits

Once Akindeju established and started executing on his two-part plan, the organization was better positioned to identify security gaps in processes and system controls. Employees grew increasingly aware of the importance of security in their ability to deliver on-time, valuable services and products, both internally and externally. Awareness drove secure execution, which, in turn, resulted in improved confidentiality, integrity and availability of systems and data.

By recruiting security champions who were already recognized leaders and influencers within the company, Akindeju created a support system that collectively spread the message of the importance of security.

The Results

While not leading with a “security first” message was more time-consuming, the approach adopted by Akindeju meant that he was better suited to put security in context of the organization’s needs and, as a result, was able to gain support and buy-in for the security and risk management programs. This backing from the top smoothed a transition to a security-aware culture.

More tangibly, as Akindeju’s workload increased, the elastic co-sourcing arrangement with external experts allowed him to demonstrate the need for full-time security staff. After a period of time, he submitted a request for internal headcount; he now has a team of four permanent FTEs and up to six contractors. Using a capability map he developed, he is planning to hire three additional FTEs. Recently, Akindeju deployed a SOC model and monitoring platform that is jointly maintained by his internal team and an external security co-sourcing partner.

In a short period of time, Akindeju was able to institute an end-to-end security culture. His success was based on his willingness to learn the business, to learn from colleagues and to educate teammates who would eventually help him with his mission. Akindeju was able to leverage the innovative, technology-driven culture already in place to help the company become a more secure and compliant technology-forward innovator (figure 3).

Akindeju is using the COBIT maturity benchmark to work through governance and reporting to ensure that his team can objectively measure progress against goals. When he started his journey at Mercury, Akindeju says the company did not have a formalized security maturity assessment framework in place. This has now changed and, working with an external firm, Mercury has set an overall maturity level 4 as its target operating state and is well on its way to achieving that objective (figure 4).

Akindeju notes marked improvement in service management, perimeter security, overall engagement and operations. These positive results have been presented to executives and the board, which is helping him clinch funding commitments that allow the security and risk team to, in Akindeju’s words, “be more proactive and introduce better processes to identify vulnerabilities, prioritize remediation, and become more strategic in meeting the security needs of the business.”
Author’s Note

Akindeju noted that he could not have achieved any success without the unflinching support of Mercury’s senior leadership team. He acknowledges Tim Aynsley, head of information and communications technology (ICT), Kevin Angland, general manager retail and digital, Graeme Hill, infrastructure asset manager, and others.

Endnotes

1 Technology risk management was brought into Akindeju’s remit in 2019 to drive enterprisewide technology risk management activities.
2 Mercury, Investor Centre, https://www.mercury.co.nz/investors

Table

<table>
<thead>
<tr>
<th>Before</th>
<th>After Introducing a Formal Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eager adoption of new technology</td>
<td>Security by design</td>
</tr>
<tr>
<td>No evident formal security consideration in implementation and delivery</td>
<td>Security through delivery</td>
</tr>
<tr>
<td>Lack of evident formal technology risk management processes</td>
<td>Implementation of security frameworks including COBIT and ISO 27001-2/5, ISO 27002, ISO 27005, and ISA/IEC 62443</td>
</tr>
<tr>
<td>Lack of ability to remEDIATE security vulnerabilities</td>
<td>Security control mapping</td>
</tr>
<tr>
<td>No formal security practice/function</td>
<td>Seven full-time security staff; elastic co-sourcing agreement with additional external experts</td>
</tr>
<tr>
<td>Low security awareness among employees</td>
<td>Formalized security training for all employees</td>
</tr>
<tr>
<td></td>
<td>Established security champions program</td>
</tr>
<tr>
<td></td>
<td>Formalized security governance</td>
</tr>
<tr>
<td></td>
<td>Ongoing capabilities assessments</td>
</tr>
</tbody>
</table>

Figure 3—A Before and After Security View of Mercury NZ

<table>
<thead>
<tr>
<th>Year</th>
<th>Eager adoption of new technology</th>
<th>Security by design</th>
<th>No evident formal security consideration in implementation and delivery</th>
<th>Security through delivery</th>
<th>Lack of evident formal technology risk management processes</th>
<th>Implementation of security frameworks including COBIT and ISO 27001-2/5, ISO 27002, ISO 27005, and ISA/IEC 62443</th>
<th>Lack of ability to remediate security vulnerabilities</th>
<th>Security control mapping</th>
<th>No formal security practice/function</th>
<th>Seven full-time security staff; elastic co-sourcing agreement with additional external experts</th>
<th>Low security awareness among employees</th>
<th>Formalized security training for all employees</th>
<th>Established security champions program</th>
<th>Formalized security governance</th>
<th>Ongoing capabilities assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td>Eager adoption of new technology</td>
<td>Security by design</td>
<td>No evident formal security consideration in implementation and delivery</td>
<td>Security through delivery</td>
<td>Lack of evident formal technology risk management processes</td>
<td>Implementation of security frameworks including COBIT and ISO 27001-2/5, ISO 27002, ISO 27005, and ISA/IEC 62443</td>
<td>Lack of ability to remediate security vulnerabilities</td>
<td>Security control mapping</td>
<td>No formal security practice/function</td>
<td>Seven full-time security staff; elastic co-sourcing agreement with additional external experts</td>
<td>Low security awareness among employees</td>
<td>Formalized security training for all employees</td>
<td>Established security champions program</td>
<td>Formalized security governance</td>
<td>Ongoing capabilities assessments</td>
</tr>
<tr>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4—Improvement in Mercury NZ Security Maturity Model

COBIT Maturity

4 Quantitative The enterprise is data driven, with quantitative performance improvement.

0 Incomplete Work may or may not be completed toward achieving the purpose of governance and management objectives in the focus area.
Cybersecurity Incident Response
Tabletop Exercises Using the Lego Serious Play Method

It is foolish to wait until an enterprise is in the midst of a data breach to test its cybersecurity incident response plan (CSIRP). How likely is it that the enterprise will know that a cyberattack is underway and be able to react appropriately? Are the enterprise’s current policies and procedures sufficient to effectively detect, respond to and mitigate sophisticated cybersecurity incidents?

The use of tabletop exercises (TTEs) can help answer these and other questions. TTEs are designed to prepare for real cybersecurity incidents. By conducting TTEs, an incident response team increases its confidence in the validity of the enterprise’s CSIRP and the team’s ability to execute it.\(^1\)

The Lego Serious Play (LSP) method can support, improve and strengthen the design, execution and outcomes of the TTEs an enterprise uses to assess the capabilities, effectiveness and maturity of its CSIRP. TTEs help determine whether the current CSIRP is able to detect, respond to and mitigate incidents in a timely and successful manner. They can also ascertain whether the right people are in place, whether they are aware of and committed to their duties during a real cybersecurity incident, and whether they can execute the procedures correctly.

Although TTEs are based on recommended methodologies, such as the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-84,\(^2\) the need to improve TTEs to prevent failures and overcome challenges has been recognized. Cybersecurity professionals need to acknowledge these shortcomings and explore new mechanisms to manage them. The LSP method has proved to be one mechanism that enriches and improves cybersecurity incident response TTEs and reduces the risk of failure.

The Value of Tabletop Exercises

A TTE presents a realistic cybersecurity incident scenario to which an enterprise must respond. Participants in the exercise describe how they would react during the incident, what tools they would use and what procedures they would follow. At the end of the exercise, the enterprise can determine where its incident response plans and policies are working well, where there is room for improvement, and how it can refine its CSIRP.

---

**Fabian Garzón, CISM, CRISC, GCIH**
Has two decades of experience in the IT and information security consultancy services working in various roles including product management, IT security operations engineer, cybersecurity incident management, Payment Card Industry Data Security Standard (PCI DSS) implementation, cyberrisk management and, now, chief technology officer at Hackergame, Colombia. He can be reached at fabian@hackergame.com or www.linkedin.com/in/r-fabian-gg/.

**Gustavo Garzón, CISM, CRISC, PMP**
Has more than 15 years of experience in technology and digital security areas as a consultant and team leader implementing information technology projects in Latin America and now is the founder and chief executive officer at Hackergame. He was a member of the development team for *A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS)*. He can be reached at gustavo@hackergame.com or www.linkedin.com/in/gustavogarzonr.
Increasingly, clients, insurers, auditors and regulators require evidence of preparedness, and the results of a TTE can satisfy these requirements.

A variety of standards, regulations and guides related to cybersecurity incident response recommends the testing of CSIRPs. Figure 1 provides a sampling of standards from NIST, PCI SSC, the SANS Institute, the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) and ISACA. The US Department of Homeland Security’s Ready Campaign, designed to educate and empower US citizens to prepare for, respond to and mitigate emergencies, summarizes the benefits and outcomes of exercises to test response plans. They include the following:

- Identify planning and procedural deficiencies.
- Clarify roles and responsibilities.
- Obtain participant feedback and recommendations for program improvement.
- Measure improvement compared to performance objectives.

- Improve coordination between internal and external teams, enterprises and entities.
- Increase awareness and understanding of hazards and the potential impact of hazards.
- Assess the capabilities of existing resources and identify needed resources.

TTEs must follow some widely accepted methodology or guide. NIST SP 800-84, for example, focuses on TTEs and functional exercises. It can help enterprises design, develop, conduct and evaluate testing, training and exercise events in an effort to assist personnel in preparing for adverse situations involving IT.

TTEs are discussion-based exercises. Personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular crisis situation. A facilitator presents a scenario and asks the participants questions related to the scenario, which initiates a discussion of roles, responsibilities, coordination and decision making. Figure 2 outlines the NIST SP 800-84 methodology for conducting a TTE.

Failures and Challenges of Tabletop Exercises

TTEs are not exempt from weaknesses and discouraging results. Disengaged staff, low attendance, inattention during the exercise and other failures have been identified. They include the following:

### Figure 1—Cybersecurity Incident Response Guidelines

<table>
<thead>
<tr>
<th>Standard</th>
<th>Requirement/Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST SP 800-53</td>
<td>Requires US federal agencies to conduct exercises or tests for their incident response capabilities at least annually</td>
</tr>
<tr>
<td>NIST SP 800-61</td>
<td>Requires that the incident response policy, plan and procedures be tested to validate their accuracy and usefulness</td>
</tr>
<tr>
<td>PCI Data Security Standard (DSS) 3.2</td>
<td>Requires the implementation of an incident response plan, including a review and test of the plan at least annually</td>
</tr>
<tr>
<td>SANS Institute</td>
<td>Recommends drills at regular intervals to ensure that all individuals on the incident response team can perform their duties during an incident</td>
</tr>
<tr>
<td>ISO/IEC 27035</td>
<td>Recommends periodic tests of the information security incident management scheme</td>
</tr>
<tr>
<td>ISACA®</td>
<td>Recommends comprehensive exercises that involve all key factors: communications, coordination, resource availability and response</td>
</tr>
</tbody>
</table>
Lack of clear and achievable objectives—Do not overcomplicate the objectives of the TTE, and make sure they are achievable.

Irrelevance—The value of a TTE is the opportunity to discuss individual interests (related to areas or roles) and to explore new and unforeseen issues.

Tedium—TTEs are a means to expand the scope of an enterprise’s human, process and technology assets. For some individuals, the prospect of a TTE meeting may not be exciting, so it is important to make the exercises interesting.

Boring scenarios—The TTE scenario should ensure that all the participants are engaged. Maintaining their interest in the conversation throughout the session can be difficult, but it can be accomplished by including issues that are specific to the participants’ areas of responsibility.

Lack of visual appeal—Pictures, short videos, manipulated images, simulated news and social media messages can create realism and keep participants engaged. Failure to present a visually stimulating experience will result in less interaction and more disengagement.

Exercises that are too challenging or not challenging enough—Achieving the right balance can be difficult. If scenarios go too far, participants may be overwhelmed by the various problems presented to them. This can lead to a reduction in active participation during the TTE. The same is true for a scenario that is too easy to handle and does not test the team.

Distractions—if TTE participants divide their attention between their electronic devices and the exercise—multitasking—neither activity gets the benefit of the brain’s full resources, and participants are likely to miss important details of the cybersecurity scenario.12

This list of failures and challenges is not all-inclusive, but these shortcomings have been highlighted because LSP addresses them directly.

Game-Based Learning and Gamification

Because many of the failures of TTEs are related to interest, interaction, engagement and participation, creative solutions are needed, and this is where game-based learning and gamification can help. An example of game-based learning applied to TTEs is Backdoors & Breaches, an incident response card game that is simple in concept, easy to play and fun.13

Gamification is the craft of deriving fun and engaging elements found typically in games and thoughtfully applying them to real-world or productive activities. Game mechanics such as points, challenges, leaderboards, rules and incentives make game-play enjoyable. Gamification applies these mechanics to motivate the audience to achieve higher and more meaningful levels of engagement.14

Many enterprises have experimented with gamification to improve end-user awareness. The results have been remarkable.15 Games have the ability to disarm people, negating their natural aversion to meetings because games make them fun, and most games are associated with the chance to win. Although using games to increase people’s engagement with work may seem counterintuitive, game playing appears to be paying off in the areas of cybersecurity awareness, incident response exercises and cybersecurity skills development.

Lego Serious Play Method

In the search for innovative and proven methods of game-based learning that can be used without any restrictions in the development and execution of TTEs and can mitigate the failures described previously, LSP is an obvious choice. In simple terms, LSP is a systematic method that enables people to use Lego bricks to solve problems, explore ideas and achieve objectives.16 Lego bricks are combined with animals,
miniature figures and an extensive selection of special elements such as wheels, tires, windows, trees, sticks, globes, spiral tubes, ladders and fences. Figure 3 shows models built with Lego pieces during an LSP exercise.

If participants’ hands are occupied with Lego pieces, one failure of TTEs—distraction—is already diminished. But LSP is much more than building models. It is a creative approach to enhancing innovation and improving business performance, with the focus on unleashing play. Based on the merging of play with organizational development, systems thinking and strategy development, LSP can lead to improved meetings, faster innovation processes, team growth and better communication.17

The purpose of LSP is to change “lean backward meetings” to “lean forward meetings,”18 where the result is more participation, more insights, more engagement, and, ultimately, more commitment and faster implementation. In several TTEs executed with LSP in Latin America in 2019, the traditional failures of TTEs were reduced. The following are some of the positive outcomes:

- Everyone involved in the TTE has an interest or stake in the agenda.
- Everyone commits to and honors decisions reached after the TTE.
- Team understanding is increased, and team frustration is decreased.
- Participants do not consider the exercises a waste of time.
- All participants share a common understanding and frame of reference (CSIRP in place).
- Conversations flow without the fear of treading on personal feelings.
- Cybersecurity incident response can be complex and multifaceted. TTEs using LSP help participants grasp the bigger picture, find connections, and explore options and potential solutions.
- Participants acquire the skills to communicate more effectively when a cybersecurity incident happens and approach their work with increased confidence and commitment.
- There is a level playing field for discussion.
- Excuses and lack of initiative are less common after the TTE.

Figure 3—Lego Models
What are the practical applications of the LSP method? Many case studies have been documented. Effective team building; shared vision, values and behaviors; and the development of workshops are some of the practical examples. Depending on the challenge (the incident scenario in the TTE), the LSP method has seven application techniques (figure 4), all of which are built on four core phases (figure 5). enterprises are strongly encouraged to adapt scenarios to use in their own incident response exercises. For TTEs executed with LSP, sample scenarios can be found in the Center for Internet Security (CIS) guide or appendix A of NIST SP 800-61. If an enterprise wants to simulate incidents using cloud-based services, Amazon Web Services (AWS) provides sample scenarios.

During TTEs applying the LSP method in Colombia’s financial enterprises, it was observed that participants with shared Lego models demonstrated a team understanding of a cyberattack, its impact and the step-by-step incident response. They had a shared vision of the response strategy and how to mitigate the simulated cybersecurity incident. Participants can make physical connections between various Lego models to demonstrate how they are related; this helps them solve problems involving cross-functional relationships within the enterprise (e.g., legal, IT, human resources, public relations) and decreases the resistance to performing cross-functional TTEs. Modifying Lego models is analogous to manipulating elements in a system, network or process in a simulated incident scenario. The participants explore “what if” questions (injecting new elements into cybersecurity scenarios) and how these elements can impact the results of their response. By observing connections among Lego model systems and by playing “what if,” participants are able to identify the underlying truths that will guide them through real cybersecurity incidents in the future.

Conclusion

A number of efforts can advance an enterprise’s CSIRP, including the development of TTEs that are fun, engaging and interactive. Lego Serious Play can be an important tool in a cybersecurity incident response TTE.

When planning a TTE, remember that people tend to be more engaged when the subject matter is pertinent, fun, appealing and challenging. It is important to test the CSIRP and the incident response team as often as possible with different scenarios, different exercises and different mechanisms.

LSP is not just for incident response TTEs. Once cybersecurity professionals understand and have practiced and tested the LSP method, they can use it for other types of workshops, including security awareness, skill building, team building, cybersecurity program goal setting, cybersecurity behavior modification and cultural activities within the community, enterprise, workplace and home.

Endnotes

8 ISACA®, Responding to Targeted Cyberattacks, USA, 2013
10 Op cit NIST, 2006
14 Chou, Y.; Actionable Gamification—Beyond Points, Badges, and Leaderboard, Octalysis Media, USA, 2017
17 Kristiansen, P.; R. Rasmussen; Building a Better Business Using the Lego® Serious Play® Method, Wiley, USA, 2014
19 Op cit Blair, Rillo
22 Op cit NIST, 2012
24 HackerGame, "Taller de ciberseguridad con Lego® Serious Play®—Cómo afrontar una Crisis Digital en tu empresa," YouTube, 15 August 2019, www.youtube.com/watch?v=iKQ0IlU9YY

Enjoying this article?

• Learn more about, discuss and collaborate on information and cybersecurity in ISACA’s Online Forums. https://engage.isaca.org/onlineforums
With the proliferation of cloud computing services available, our organization is considering moving IT-related services to cloud-based services. What are the benefits and risk associated with using cloud services? What steps should we follow when selecting a cloud service provider (CSP)?

In the early days of cloud computing, a cloud symbol was used to represent computers placed on networks out of the boundary of organization. This is likely the origin of the term “cloud computing” for the services available through the Internet. Based on the type of services offered, there are different types of cloud services available, and organizations should consider which model is most suitable for their business.

Primarily, cloud computing is an outsourcing service model and has become popular due to multiple benefits organizations can derive from using cloud-based services. Those benefits include:

- **Scalability**—CSPs offer scalable computing environments and often include pay-as-you-use models, which help organizations handle increased volumes of data processing without investing in nonproductive computing capacity and without impacting performance.
- **Affordability**—Organizations need not invest in costly infrastructure and incur costs for maintaining that infrastructure. CSPs offer the required computing capability on a subscription model and help save on capital expenditures, particularly for small- and medium-sized organizations.
- **Lower capital costs**—Organizations can provide unique services using large-scale computing resources from CSPs, and then nimbly add or remove IT capacity to meet peak and fluctuating service demands while only paying for actual capacity used.
- **Lower IT operating costs**—Organizations can rent added server space for a few hours at a time rather than maintain proprietary servers without worrying about upgrading their resources whenever a new application version is available. They also have the flexibility to host their virtual IT infrastructure in locations offering the lowest cost.
- **Improved operations**—Organizations can reduce the need to handle hardware or software installation or maintenance.
- **Improved business continuity planning (BCP)/disaster recovery (DR) infrastructure**—Organizations can leverage the process to create more robust disaster recovery and business continuity features and services, if properly managed.
- **Higher efficiency**—Organizations may be able to optimize their IT infrastructure and gain quick access to the computing services required.

While acknowledging the benefits of CSPs, like any other technology innovation, cloud services also have associated risk. The Cloud Security Alliance (CSA) has identified the top threats for cloud services:

1. Data breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access and key management
5. Account hijacking
6. Insider threat

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, CDPSE, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.
7. Insecure interfaces and application programming interfaces (APIs)
8. Weak control plane
9. Meta-structure and appli-structure failures
10. Limited cloud usage visibility
11. Cloud services are also prone to attacks

These threats may result in any of the following negative consequences for organizations using cloud services:

- **Loss or theft of IP**—Some of an organization’s most valuable data, IP, may be lost or stolen.
- **Noncompliance and regulatory actions**—Organizations need to comply with laws and regulatory controls, for example the US Health Insurance Portability and Accountability Act (HIPAA) for private health information, the US Family Educational Rights and Privacy Act (FERPA) for confidential student records, and some countries prohibit storing and processing resident information out of geographical boundaries. Organizations must be aware of the location of their data, who can access it and what is the level of protection. Although CSPs are responsible, organizations are accountable for compliance.
- **Loss of control over end user actions**—End users need to access data in the cloud and, with bring your own device (BYOD) and mobile workforces, many organizations risk losing control over the actions of authorized end users.
- **Malware infections that unleash a targeted attack**—Cloud services can be subject to targeted attacks resulting in data breaches. Successful attacks diminish trust and can negatively impact the reputation of an organization.
- **Contractual breaches with customers or business partners**—Contracts between organizations and CSPs should control the data flow, processing and dissemination to authorized users. Since it is another vendor relationship, contracts with CSPs must be carefully drafted and agreed on in all cases.
- **Reduced level of security**—Information security in the cloud may not be required by the organization policy. Although the CSA has defined security guidelines, getting assurance via periodic audits may be a challenging task for the organization.

**How to Proceed?**

Organizations that wish to subscribe to CSPs by third party need to consider the following:

- Outsourcing decisions are strategic and, as such, must be included in the overall outsourcing strategy.
- An organization-level service provider management framework and policy need to be in place.
- A central vendor management steering committee can help in addressing risk.
- Selecting a CSP must be done carefully since it may not be easy to switch the vendor in the future.
- Each service provider has unique risk factors, which means it is prudent to study the practices followed by each service provider.
- Organizations that wish to use cloud services need to have clearly defined functional and security requirements.
- The contract with a CSP must include a “right to audit” clause, and the organization must have a mechanism to execute periodic audits of vendors. Most CSPs may not agree to audits by the organization’s auditor but may agree to a shared audit report. The organization must insist on SOC reports using the SSAE 18 standard by approved auditors.
- Define and monitor service level agreements.

Cloud computing is here to stay. Organizations need to manage the risk associated with hosting sensitive data offsite, which will strengthen confidence with the service provider and allow the organization to reap the benefits of using a cloud platform.

**Endnotes**

ACROSS

1 Consumer credit reporting agency subject to a major security breach in 2017
5 Procedures to protect electronic data from unauthorized access or use
9 Protocol for file transfer, abbr.
10 Duties and responsibilities
11 With no exceptions
12 Permit
13 It may serve as a model
15 Are situated
17 Center, abbr.
18 Speculate about a future result
19 Arena shout
20 Where many inspections are done, 2 words
22 Accountant
25 Large tree
27 It may be poured on troubled waters
28 Noted "Talks"
29 Radio band
31 ___ plan, proposed strategy
32 Reveal
36 Gifted foresight
38 Net alternative
40 Web inventor, first name
41 Conclusion regarding the purpose of the cyberattack on 1 Across
42 Type of software that advocates adaptive planning and continual improvement
43 Figure out
44 Ordered reference standard
45 Web

DOWN

1 Secretly steal data
2 Not protected by a fix for a security flaw
3 Guaranteed against failure
4 Programming language
5 Fort Knox bar
6 Physical fitness
7 Range or extent, of an IT audit, e.g.

8 Kind of analysis
14 Setback
16 ISACA's concern
18 Zone
21 Kind of support
22 One of the five attributes of an audit finding
23 Transcendental number
24 COBIT 2019 audit report component, ____ goals
26 Lessen the seriousness or extent of a crime or disastrous event
30 .001 inch
32 Early operating system
33 Push
34 A, in Acapulco
35 Objectives
37 Maintain, as some tools
38 C-suite members
39 Trial phase

Answers on page 58
TRUE/FALSE

ALVERO AND MCCARTHY ARTICLE
1. One of the categories of common automation project pitfalls is authentication of bots, which results from a lack of control ensuring bot functionality and issue resolution.
2. Although robotic process automation (RPA) is traditionally considered an approach to handling repetitive, routine tasks—often categorized as “low value”—internal audit’s role should be to ensure that the organization does not invest in automating tasks that are truly ineffective or of low value.
3. A survey of information workers revealed that one quarter of those employees believe their jobs could be replaced by automation.

PEARCE AND KETCHEN ARTICLE
4. Now more than ever, humans are desirable data subjects, whether or not they know they are serving in that capacity—a situation the EU General Data Protection Regulation (GDPR) addresses through its informed consent requirements.
5. Four ethical principles should inform the standards of organizations that sell or leverage data: respect for autonomy, beneficence, nonmaleficence and protection.
6. Among the top-rated medical applications (apps) for Android, 46 percent shared user health data with third-party organizations, and entities from 79 organizations used or consumed the data in some way.

QURESHI ARTICLE
7. Auditors can use the Emerging Technology Analysis Canvas (ETAC), which focuses on four conditions—opportunity/trigger, impact, feasibility and future—to identify and assess the risk of emerging technologies.
8. Artificial intelligence (AI) uses complex algorithms to propose decisions based on a pattern or learned over time. Because those algorithms are invisible, auditors must focus on factors such as the logical flow of processes, unintended bias and review/approval of algorithm output.
9. ISACA’s blockchain-oriented audit program focuses on six categories: pre-implementation, governance, development, security, census and privacy.

GOMEZ AND HINLEY ARTICLE
10. Nonmedical information attached to a medical file and medical information used for marketing purposes may fall in the gap between the US Health Insurance Portability and Accountability Act (HIPAA) and the US State of California Consumer Privacy Act (CCPA) requirements.

11. The CCPA’s requirements around third-party notification exactly mirror the requirements of HIPAA.
12. Organizations should create a new privacy statement, which would include a comprehensive list of the third parties to whom the organization sells personal information, to comply with CCPA requirements that are over and above HIPAA requirements.

SHARMA AND MUKHOPADHYAY ARTICLE
13. Assessing and mitigating the risk of a distributed denial-of-service (DDoS) attack in the gaming industry involves computing the risk of not detecting a DDoS attack and the severity of such an attack, creating a risk and severity heat map of undetected attacks, then considering options for reduction and transfer of risk.
14. The approach described in the article groups types of DDoS attacks into five categories and suggests steps to produce classification accuracy to at least 80 percent.
15. Suggested risk mitigation strategies include adding stringent firewalls and intrusion detection systems (IDSs), diverting excess or illegitimate traffic to backup servers or content delivery networks (CDNs), and transferring residual risk to cyberinsurance policies.

SEEDAT ARTICLE
16. One of the lessons learned from the software-defined networking in a wide area network (SD-WAN) project described in the article is the need for a project charter that includes, at the least, project objectives and deliverables, in-scope items, exclusions, assumptions, high-level timelines, and responsible parties.
17. Past project experience indicates that project teams should ensure that the latest stable and compatible version of the operating system (OS) is implemented. It is not necessary to update patches before adding apps or configuring services to the system.
18. Although it will be necessary when the system goes live, it is not critical to mask sensitive data and restrict/protec access to sensitive data during the testing phase.

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current Journal subscribers. Take the quiz online at www.isaca.org/cpequiz, where it is graded automatically. You will be responsible for submitting your credit hours at year-end for CPE credits. A passing score of 75 percent will earn one hour of CISA, CRISC, CISM or CGEIT CPE credit.
ISACA Member and Certification Holder Compliance

The specialized nature of information systems (IS) audit and assurance and the skills necessary to perform such engagements require standards that apply specifically to IS audit and assurance. The development and dissemination of the IS audit and assurance standards are a cornerstone of the ISACA® professional contribution to the audit community.

IS audit and assurance standards define mandatory requirements for IS auditing. They report and inform:

- IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession’s expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor® (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder’s conduct by the ISACA Board of Directors or appropriate committee and, ultimately, in disciplinary action.

ITAF™, 3rd Edition (www.isaca.org/itaf) provides a framework for multiple levels of guidance:

IS Audit and Assurance Standards

The standards are divided into three categories:

- General standards (1000 series)—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated.

Please note that the guidelines are effective 1 September 2014.

General

1001 Audit Charter
1002 Organizational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency
1007 Assertions
1008 Criteria

Performance

1201 Engagement Planning
1202 Risk Assessment in Planning
1203 Performance and Supervision
1204 Materiality
1205 Evidence
1206 Using the Work of Other Experts
1207 Irregularity and Illegal Acts

Reporting

1401 Reporting
1402 Follow-Up Activities

IS Audit and Assurance Guidelines

The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorization as the standards (also divided into three categories):

- General guidelines (2000 series)
- Performance guidelines (2200 series)
- Reporting guidelines (2400 series)

General

2001 Audit Charter
2002 Organizational Independence
2003 Professional Independence
2004 Reasonable Expectation
2005 Due Professional Care
2006 Proficiency
2007 Assertions
2008 Criteria

Performance

2201 Engagement Planning
2202 Risk Assessment in Planning
2203 Performance and Supervision
2204 Materiality
2205 Evidence
2206 Using the Work of Other Experts
2207 Irregularity and Illegal Acts
2208 Sampling

Reporting

2401 Reporting
2402 Follow-Up Activities

IS Audit and Assurance Tools and Techniques

These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programs, reference books and the COBIT® 5 family of products. Tools and techniques are listed under www.isaca.org/itaf.

An online glossary of terms used in ITAF is provided at www.isaca.org/glossary.

Prior to issuing any new standard or guideline, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director, Content Strategy, via email (standards@isaca.org); fax (+1.847.253.1755) or postal mail (ISACA International Headquarters, 1700 E. Golf Road, Suite 400, Schaumburg, IL 60173, USA).

Links to current and exposed ISACA Standards, Guidelines, and Tools and Techniques are posted at www.isaca.org/standards.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of these products will assure a successful outcome. The guidance should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the control professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or IS environment.
Grow Your Knowledge

Explore ISACA’s expert-developed resources for wisdom, guidance and real-world experiences to help you achieve your goals in your organization.

IT governance is more important than ever in achieving digital transformation and driving value. ISACA recently updated the content outline for its Certified in the Governance of Enterprise IT (CGEIT) certification exam to reflect the needs of this evolving landscape. Browse our new CGEIT certification publications and other governance-related resources in the pages ahead.

ISACA Resources
for guidance and professional development
The **CGEIT Review Manual 8th Edition** is designed to help individuals prepare for the CGEIT exam and understand the responsibilities of those who implement or manage governance of enterprise IT (GEIT) or have significant advisory or assurance responsibilities in regards to GEIT. It is a detailed reference guide that has been developed and reviewed by subject matter experts actively involved in GEIT worldwide.

The manual is organized to assist candidates in understanding essential concepts and studying the following updated job practice areas:

- **GOVERNANCE OF ENTERPRISE IT**
- **IT RESOURCES**
- **BENEFITS REALIZATION**
- **RISK OPTIMIZATION**

The **CGEIT Review Manual 8th Edition** features an easy-to-use format. Each of the book’s four chapters has been divided into two sections for focused study. Section one of each chapter contains the definitions and objectives for each of the CGEIT® practice areas. It also includes:

- Self-assessment questions and explanations of the answers
- Suggested resources for further study

Section two of each chapter consists of content and reference material that supports the knowledge subdomains for each job practice area. The material enhances CGEIT candidates’ knowledge and/or understanding when preparing for the CGEIT certification exam. In addition, the **CGEIT Review Manual 8th Edition** includes definitions of terms most commonly found on the exam.

The manual is excellent as a stand-alone document for individual study or as guide or reference for study groups and chapters conducting local review courses, and it can be used in conjunction with the:

- **CGEIT Review Questions, Answers & Explanations Manual 5th Edition**
- **CGEIT Review Questions, Answers & Explanations Database – 12 Month Subscription**
CGEIT Questions Answers and Explanation Manual, 5th Edition

Print Product Code: CGQ5ED | Member Price: $72 | Non-member Price: $96

The CGEIT Review Questions, Answers & Explanations Manual, 5th Edition is designed to familiarize candidates with the question types and topics featured in the CGEIT exam. The manual consists of 300 practice items. These questions are not actual exam items but are intended to provide CGEIT candidates with an understanding of the type and structure of questions and content that has previously appeared on the exam. This publication is ideal to use in conjunction with the CGEIT Review Manual 8th Edition.

To help candidates maximize—and customize—study efforts, questions are presented in the following two ways:

- Sorted by job practice area—questions, answers and explanations are sorted by the CGEIT job practice areas. This allows the CGEIT candidate to refer to questions that focus on a particular area as well as to evaluate comprehension of the topics covered within each practice area.

- Arranged as a sample 75-question exam—The 75 questions are arranged in the same percentages as the current CGEIT job practice areas. Candidates are urged to use this sample test to simulate an actual exam and to determine their strengths and weaknesses in order to identify areas that require further study. Answer sheets and an answer/reference key for the sample exam are also included. All sample test questions have been cross-referenced to the questions sorted by practice area, making it convenient for the user to refer back to the explanations of the correct answers.

CGEIT Review Questions, Answers & Explanations Database—12 Month Online Subscription

eBook Product Code: EPUB_CSXG2 | Member Price: $60 | Non-member Price: $65
Web Download Product Code: WCSXG2 | Member price: $50 | Non-member price: $55

CGEIT® Review Questions, Answers & Explanations Database—12 Month Subscription is a comprehensive 300-question pool of items that contains the questions from the CGEIT® Review Questions, Answers & Explanations Manual, 5th Edition. The database is available via the web, allowing CGEIT candidates to log in at home, at work or anywhere they have Internet connectivity, and is MAC and Windows compatible.

Exam candidates can utilize an interactive planner to build a custom study plan, and a personalized dashboard serves as the primary method to navigate studies and track progress. Candidates will take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas.

Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CGEIT candidates to identify their strengths and weaknesses and focus their study efforts accordingly. Other features provide the ability to select sample exams by specific job practice domain, view questions that were previously answered incorrectly and vary the length of study sessions, giving candidates the ability to customize their study approach to fit their needs.
Over the years, best-practice frameworks have been developed and promoted to assist in the process of understanding, designing and implementing enterprise governance of IT (EGIT). COBIT® 2019 builds on and integrates more than 25 years of development in this field, not only incorporating new insights from science, but also operationalizing these insights as practice.

**COBIT 2019 Framework: Introduction and Methodology** updates COBIT principles while laying out the structure of the overall framework.

- New concepts are introduced and terminology is explained—the COBIT Core Model and its 40 governance and management objectives provide the platform for establishing your governance program
- The performance management system is updated and allows the flexibility to use maturity measurements as well as capability measurements
- Introductions to design factors and focus areas offer additional practical guidance on flexible adoption of COBIT 2019, whether for specific projects or full implementation

From its foundation in the IT audit community, COBIT has developed into a broader and more comprehensive information and technology (I&T) governance and management framework and continues to establish itself as a generally accepted framework for I&T governance.

COBIT is a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise. Enterprise I&T means all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise.

COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure. This publication also includes detailed information about each of the components relevant to each governance and management objective.
Let Everyone Know You’re a Technical Privacy Pro

Show the world you bring in-depth knowledge and experience in privacy by design with ISACA®'s new technical privacy certification, Certified Data Privacy Solutions Engineer™ (CDPSE™).

Early adoption of the certification is open now. Learn more: www.isaca.org/CDPSE-jv4
Join us in creating a Healthy Digital World that’s safe, secure and accessible for ALL.

www.oneintech.org