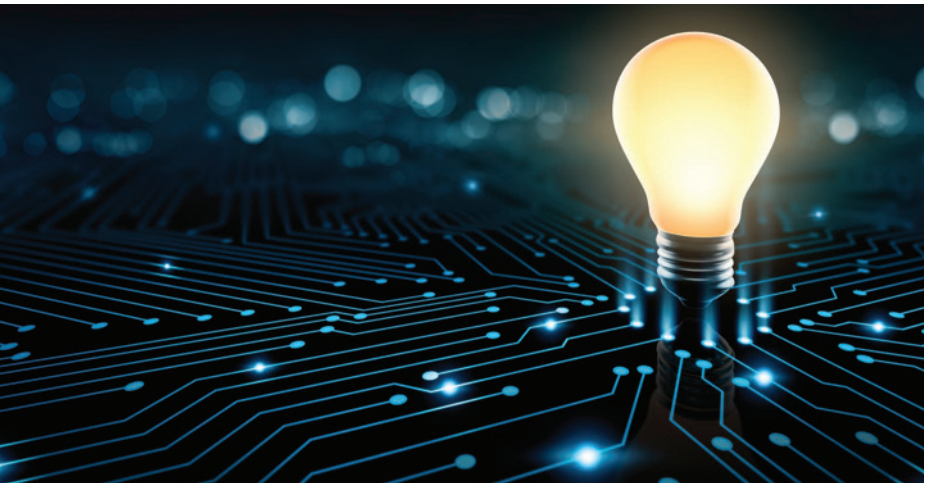
# Convergence: Where Next?

I have had the occasion recently to give some thought to what ISACA® represents and the journey over more than 50 years to get where we are today. At first, it was an association of those we would now call IT auditors.[1] Today's ISACA still welcomes IT auditors as well as professionals in information security, risk management, data privacy, IT governance and other specialties. This is representative of what I see as a broader convergence of control-related disciplines, which in the past I have referred to as the Control Community.

Certain questions come to my mind: Is this convergence a good thing or bad? (Spoiler alert: It is a good thing.) What does this trend mean for information security professionals? How can organizations maximize the value of convergence?

## Benefits and Drawbacks of Control Function Convergence

It is hard to argue that the movement toward aggregation of related interests is anything but a natural progression. Clearly, all the specialties need to have awareness of risk. Security—interpreted as the restriction of the use of information resources to intended purposes—is a key objective of all IT controls. Privacy depends on security; everything in IT depends on governance; and IT auditors provide assurance to all the others that the controls are in place and effective.



But does this convergence of specialties enhance or vitiate the effectiveness of each of them individually? The answer depends on whether IT control is a zero-sum game, in which the allocation of resources to one function results in the diminution of budget for the others. I have never been a chief financial officer (CFO) nor served on a budget committee, but I can well imagine a discussion in which the budgets for, say, the chief privacy officer (CPO) and the chief information security officer (CISO) are balanced against each other.

The budgetary decision may depend on a contraction. Does the organization need to build security *and* privacy? IT auditing *and* risk management? Contrarily, should those "ands" be replaced by "ors"? In other words, are the various types of controls complementary or cumulative? I am sure I do not have to say it, but to be clear, I believe that to shortchange even one aspect of information systems control is tantamount to saying that it is acceptable for there to be a hole in only one end of a boat.

## The Effect of Convergence on Information Security

I see information security standing apart from the other specialties in several ways. More than the others, it deals in the most technical aspects of control. Although information security is usually responsible for controls that are not directly embedded in the technology itself (policy and awareness come to mind), it is instrumental in many aspects of an enterprise's technological infrastructure. The function may have key roles in the acquisition, implementation and execution of software and hardware. It may be critical in the approach generally known as role-based access control (RBAC). It gets deep into system internals. And it is on the front line in responding to incidents and attacks.

**STEVEN J. ROSS** | CISA, CDPSE, AFBCI, MBCP

Is executive principal of Risk Masters International LLC. He has been writing one of the *Journal's* most popular columns since 1998. Ross was inducted into the ISACA® Hall of Fame in 2022. He can be reached at stross@riskmastersintl.com.

So, do outreach and alliance with related functions pull information security away from its core responsibilities? Dispassionately, I must conclude that, at times, it does. I have attended meetings in which a risk manager has argued in favor of implementing controls across a broad front while the CISO was trying to focus attention on defense against cyberattacks. Naturally there is a need for some give and take, but what is the CISO giving up? More to the point, what is he or she taking home?

The answer is that information security professionals need to consider what they do in the broader context of the businesses they serve. They may not always agree with the risk manager[2] or the IT auditor, but their differences are far outweighed by their common perspectives. Information security has the responsibility for aspects of the technology, but the convergence of interests with the other control specialties leads to achieving greater value from the tools they implement. They do not have to agree on everything as long as they are shoulder to shoulder on the big things.[3]

## Maximizing the Value of Convergence

If it is accepted that the mutuality of interest among control specialties, including information security, strengthens them all, what should an enterprise do to maximize the value of this convergence?

I propose that enterprises cease fragmenting the various specialties into different organizational units whose interests are not nearly so integrated. While differences exist from company to company, agency to agency, in most cases information security is encompassed in the IT function. IT auditing, of course, is in the general audit function. Privacy is often found in the office of the general counsel. And risk management is, in many cases, a part of the finance organization.

While the related specialties may be converging, their individual managers may well find themselves in contention. Buy more technology! Spend less! Keep it safe! Keep it legal! And check every box! Okay, maybe a little overstated but, for certain, the security and control of information systems is not the primary *raison d'être* of any of the functions to which they report. I suggest that it is high time to create an organizational unit that I will tentatively call IT Controls. It would institutionalize the convergence that is happening even without an organizational home.

Information security has the responsibility for aspects of the technology, but the convergence of interests with the other control specialties leads to achieving greater value from the tools they implement.

Alright, the gauntlet has been officially thrown.[4, 5] I can hear the objections already:

- **Privacy needs to be in the legal department because it is primarily a legal issue.** Actually, data privacy is a social responsibility for any organization that maintains personal identifiable information (PII) databases, whether or not there are no privacy laws.[6]
- **IT auditing needs to be in the internal audit department because it needs its independence.** Let us distinguish between organizational structure and functional autonomy. An IT auditor need not report to someone with the title of chief audit executive (CAE) to bring an unbiased and professionally skeptical perspective to the job.
- **Risk management needs to report to…well, there is really no consensus.** Some say the function should report to the board of directors[7] or the chief executive officer (CEO)[8] or the CFO[9] or the chief operating officer (COO).[10] So, if there were to be a consolidated IT Controls function, this would probably be the most reasonable reporting relationship.
- **Information security needs to report to the chief information officer (CIO).** I am familiar with several organizations in which information security is deliberately located outside of IT, specifically for reasons of independence.[11] Some advocate that the CISO should be a peer with the CIO and not in a reporting relationship at all.[12]

So why not a separate home for all IT control functions?

**LOOKING FOR MORE?**

- Read *Digital Trust: A Modern Day Imperative. www.isaca.org/digital-trust-modern-day-imperative*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

## Endnotes

1 This was the EDP Auditors Association (EDPAA). I was the first association president in office who was not an EDP auditor at the time. I had already begun my career in information security.

2 I wrote about this sort of divergence quite a few years ago in this space and concluded that in even the strongest relationships, there is room for some differences of opinion. I wrote, "It is at this point that the risks and rewards of the organization need to be considered as a whole, in context." Ross, S. J.; "The Mayor and the Sherriff," *ISACA® Journal*, vol. 5, 2010, *https://www.isaca.org/archives*

3 My wife supports for the Montreal Canadiens in the National Hockey League (NHL) and I am a die-hard New York Rangers fan. If we can survive this, information security professionals can get over a few differences of opinion with related disciplines.

4 This is not the first time I have voiced institutional heresy. In 2016, I wrote an article stating that organizations need a chief cyber officer, independent of and equal to the CIO and the CISO. I received much criticism. Ross, S. J.; "Chief Cyber Officer, *ISACA Journal*, vol. 4, 2016, *https://www.isaca.org/archives*

5 I am finding more and more organizations, including my own US State of New York, going down the chief cyber officer path. New York State, "Governor Hochul Appoints New York State's First Ever Chief Cyber Officer," USA, 27 June 2022, *https://www.governor.ny.gov/news/governor-hochul-appoints-new-york-states-first-ever-chief-cyber-officer*

6 Ross, S. J.; "Why Do We Need Privacy Laws?" *ISACA Journal*, vol. 5, 2019, *https://www.isaca.org/archives*

7 Patel, A.; "Governance and Organizational Positioning of Effective Risk Management Functions," LinkedIn, 1 October 2017, *https://www.linkedin.com/pulse/governance-organizational-positioning-effective-risk-management/*. To be fair, Patel also says that it would be okay for the risk manager to report to the CEO.

8 International Association of Risk and Compliance Professionals (IARCP), "The Chief Risk Officer," *https://www.chief-risk-officer.com/*. The IARCP also says the chief risk officer (CRO) should "have direct access to the board."

9 Quinley, K. M.; "Risk Management: Where Does It Belong?" *Med Device Online*, *https://www.meddeviceonline.com/doc/risk-management-where-does-it-belong-0001#top*. Quinley says that "[M]ost risk officers seem to report to either a CFO, a treasurer, or a vice president of finance," and he allows that they may also report to legal or safety departments.

10 Marks, N.; "Revitalizing Risk Management Through a Changed Reporting Structure," CMSWIRE, 21 July 2021, *https://www.cmswire.com/information-management/revitalizing-risk-management-through-a-changed-reporting-structure/*

11 Johnson, J. T., "Five Ways to Improve the CIO-CISO Relationship," *TechTarget*, 19 October 2021, *https://www.techtarget.com/searchcio/tip/5-ways-to-improve-the-CIO-CISO-relationship*

12 Staff, "Why CISOs Shouldn't Report to CIOs in the C-Suite," *Security Intelligence*, 21 December 2021, *https://securityintelligence.com/posts/why-cisos-shouldnt-report-to-cio-c-suite-conflict/*