

Once you have gotten past the first few months, you will be presented with several important decisions, like how to organize your team. Attendees will hear several approaches to handling critical security functions such as governance, operations, privacy, and incident investigations. There are so many ways to integrate information security responsibilities into the organization, and security officers are meeting the modern day challenges by evolving their program into a more decentralized group spread across various business units.

## Agenda

---

**Assigning Security Functions & Roles**

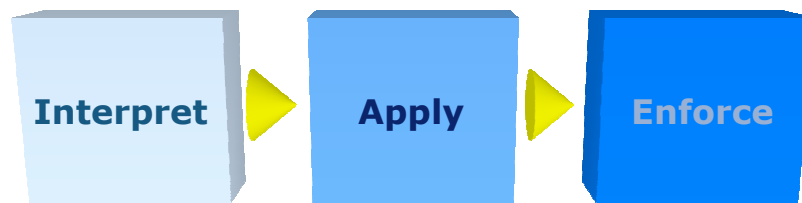
**Organizational Approaches**

**Reporting Structure**

**Doing More with Less**

## Security Team's Responsibilities

- Interpreting, applying, and enforcing security directives
- Provide an oversight role
- More like an internal consultant to the organization



3

You should really approach an information security program as if they are consultants hired to help guide the business. The majority of your time should be spent interpreting security policies & standards, and helping the organization understand how and when to apply them. If you are spending all your time with enforcement, then either the educational aspects of your program are failing or you don't have the necessary support from the leaders in the organization.

A major component of your security program will be identifying areas of the organization that don't meet internal policies and standards, assessing the risk of non-compliance, and working with the business owners to address the risks. This constant review should be a major part of your Information Security Risk Management program. As it sounds, this is the process of ensuring that established security standards are being followed and identifying any gaps, not ensuring 100% compliance. The goal is to identify high risk areas for your organization, and help them prioritize remediation efforts. The more you can distance yourself from each risk personally, and try to focus on the mission of the organization, the better chance you will have balancing out the various pulls on resources.

These days it is becoming less common for the security team to have a staff of operational/technical engineers managing and monitoring security devices, especially in medium to small size organizations. The role of a security manager is evolving more into a governance and oversight focus. Provide guidance and tools for the existing operational teams to perform their daily function, and regularly assess their effectiveness, but don't feel like you need to have your team's hands on every security related function.

## Security Functions

- Non-Technology Functions
  - Training & Awareness
  - Policy Development
- Technical Operations
  - Identity & Access Management
  - Network Security Administration
- Security Services
  - Security Risk Management
  - Incident Management
- Enforcement
  - Regulatory & Standards Compliance



4

Information Security has a broad set of responsibilities, ranging from training & awareness to digital forensics. Given this wide range of job roles, there are many ways to organize your team. You can look at breaking out the team in several different ways, for example by organizing the team into the four categories shown above, it aligns both the skills and the primary functions of the team members.

Looking at it this way, it is also easy to find functions that can be distributed to other functional groups outside of the direct security team. For example, the IAM function can easily be performed by an IT operations team, or training content may be developed by the security but presented by fulltime trainers.

# Information Security Roles

IT Security EBK: A Competency and Functional Framework		IT Security Roles																					
		Executive			Functional					Corollary													
		Chief Information Officer	Information Security Officer	IT Security Compliance Officer	Digital Forensics Professional	IT Systems Operations and Maintenance Professional	IT Security Professional	IT Security Engineer	Physical Security Professional	Privacy Professional	Procurement Professional												
Competency Areas	1 Data Security	M	M	D	E			I	E		M	D		D									
	2 Digital Forensics			M	D					M	D												
	3 Enterprise Continuity	M	M		E					I	D												
	4 Incident Management	M	M	D	E					I	D												
	5 IT Security Training and Awareness	M	M		E																		
	6 IT Systems Operations and Maintenance																						
	7 Network and Telecommunications Security																						
	8 Personnel Security	M	M		E																		
	9 Physical and Environmental Security	M	M		E																		

Source: IT Security EBK - A Competency and Functional Framework for IT Security Workforce Development  
[www.us-cert.gov/ITSecurityEBK/EBK2008.pdf](http://www.us-cert.gov/ITSecurityEBK/EBK2008.pdf)



Another way to look at organizing your security team is to look at different security competencies and map those to job roles. For example, the U.S. Department of Homeland Security has developed this matrix which is organized by 4 different functions:

- 1.Manage:** Functions that encompass overseeing a program or technical aspect of a security program at a high level, and ensuring currency with changing risk and threat environments.
- 2.Design:** Functions that encompass scoping a program or developing procedures, processes, and architectures that guide work execution at the program and/or system level.
- 3.Implement:** Functions that encompass putting programs, processes, or policies into action within an organization.
- 4.Evaluate:** Functions that encompass assessing the effectiveness of a program, policy, process, or security service in achieving its objectives.

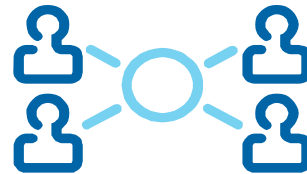
This provides a great guide for HR and hiring managers when writing new job descriptions, and can be a good reference of possible responsibilities when making organizational decisions.



For example, the CISO is responsible for overseeing and designing the forensics function, but would also responsible for evaluating the effectiveness of the incident management function. This highlights a key flaw with the matrix, in that it doesn't represent the essential role of the CISO as being the coordinator during major security breaches.

## Management Approaches

- **Centralized**
  - Allows for specialization
  - Operational / technical focus
  - Time spent on people management
- **Decentralized**
  - Conflict of interests
  - More focus on governance
  - Leader vs. just a manager
- **Hybrid**
  - Mostly security part-timers
  - Cost savings
  - Training can be a challenge



7

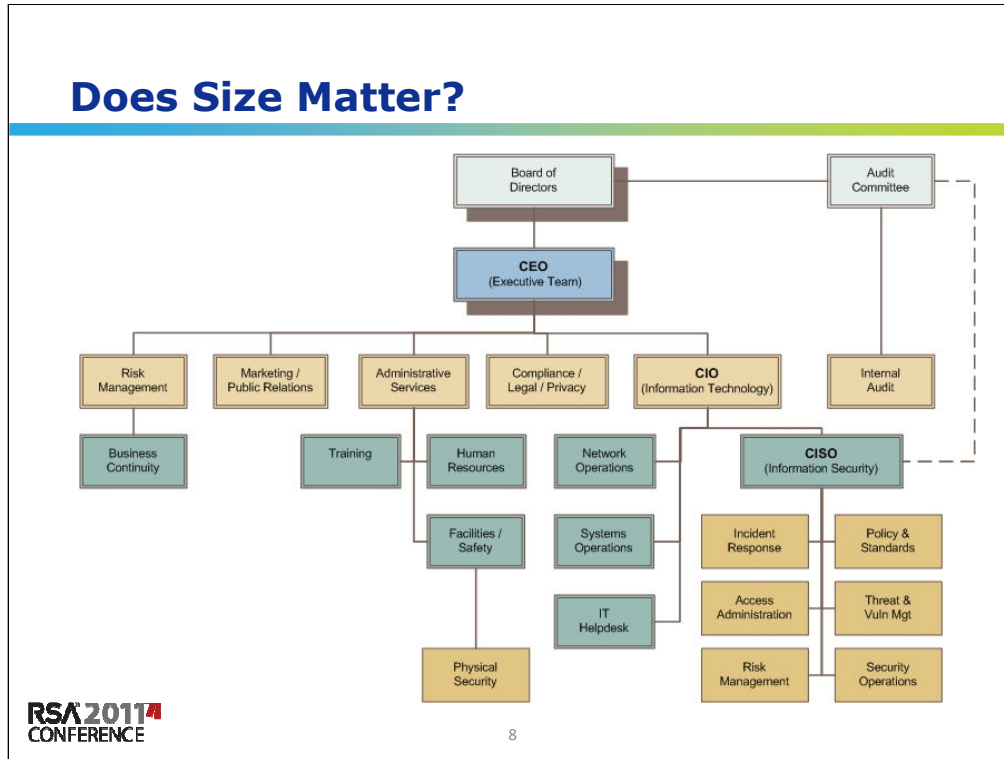
A centralized security function allows for specialization because there are usually more staff members, so people can focus on incident response, IDS traffic analysis, or maybe training & awareness, however, with a larger team you will spend more time managing people and less time doing hands-on security work. Let's face it, in some organizations even incident handling can be a fulltime job.

With a decentralized approach, you are more likely to focus on governance, but you still spend a lot of time managing the politics of getting resources from other functions to carry out the work. The resources you rely on don't directly report to you, so you have to be more of a leader than a manager in order to motivate and inspire.

The hybrid approach is a cross between the two, and can often be the most effective in medium and small sized organizations. In this model, you have resources that are only partially allocated to security work, so you end up having to compete with other objectives. But this is easier to sell to senior management, because it is a less expensive option. Getting the proper training and keeping these resources current can be a struggle however.

Turnover is the enemy of investment in training for security staff. You sink a lot of time and money into training someone to perform specialized security roles, only to have them leave for a better position at another company. With each of these three approaches, it can be challenging to keep skills current, and avoid turnover as their skills become more marketable.

## Does Size Matter?



Security leaders should be careful not to be seen as trying to build their own empire of security staff. When the size of the security team starts to dwarf some equally critical functions, you are just putting your team at risk for an undesirable level of scrutiny. With that said, the demands on the security function certainly aren't decreasing, so it can be challenging to reconcile these facts.

This shows one example of a possible reporting structure for the security team and some other related functions within the organization.

Depending on the size of your organization you may be dealing with a jack of all trades IT person who is stuck with security as one part of their responsibilities, all the way up to large organizations with several departments under the CISO specializing in everything from security architecture to access administration. Many organizations have dedicated Security Operations Centers staffed with security analysts 24/7, or mobile forensic teams. Even teams of security application testers or red teams on staff. This will somewhat depend on the mission of your organization, which functions you choose to build out and staff fulltime, versus rely on other functions within the organization.

## Who's the Boss?

- Information Technology (CIO)
  - Possible conflict of interest
  - Focus on operations / uptime / responsiveness
  - Functions closely aligned
- Facilities & Safety
  - Mission closely aligned
  - Culture gap
  - Budget Constraints
- Risk Management (Chief Risk Officer)
  - Strategic focus
  - Broad view across functions
  - No operational responsibility

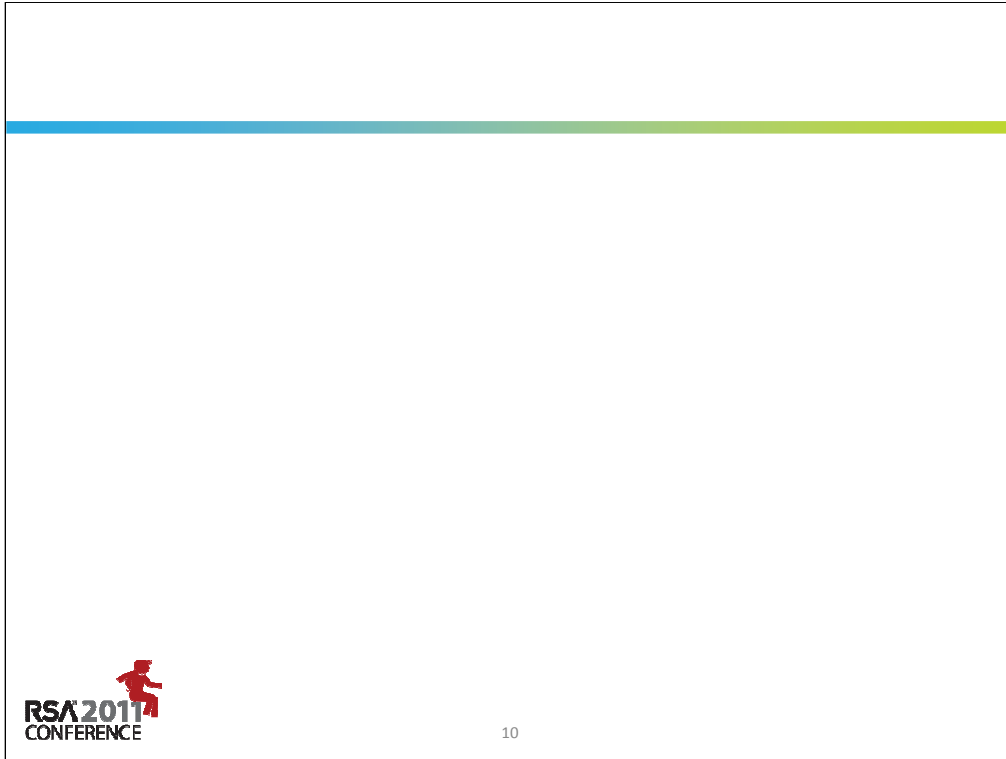


9

Does it really matter who you report to? CIO, CTO, COO, CEO, is it all the same?

Sometimes in the organizations where the IT function reports into the CFO, this can be to your advantage from a budget perspective. More commonly you will find that the information security function will report into the CIO as it grew out of the IT function. This can present a conflict of interest for the CIO when security controls are required that increase the complexity of operations, requires additional downtime for remediation, or slows responsiveness of systems. The upside is that the security team works more closely with the IT team than almost any other function including compliance and legal, so having a common boss and peer relationship can help to improve relationships if everyone feels like they are part of the same team.

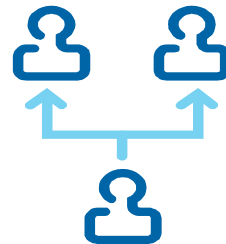
Several functions including physical security, personnel security, and safety are closely aligned with the missions of information security. Mostly this comes into play during investigations that have a physical component, but can include security offices and data centers, or protecting senior executives travelling abroad. One of the challenges is that the backgrounds for physical personnel are very different than most information security professionals. You are more likely to find former military or law enforcement in the physical security teams. The same is often true for digital forensic staff, so this is a possible alignment point. In terms of reporting into this group, it is not desirable for budget reasons. The facilities function's budget rarely increases over time, and the cost of maintaining growing information security demands can be at odds.



So far not often implemented, is the CRO role. Having security not just under this heading, but tightly integrated into this group is strategically very forward thinking. Risk management at an enterprise level has a very broad view of issues and concerns across the organization, which means that any security risks will always be rightly compared to exposures in other domains, and hopefully appropriately balanced. It also tends to deemphasize the operational side of security, instead delegating that to other teams.

## How Many Dotted Lines is too Many?

- Direct Reporting
  - Audit Committee, Board of Directors
  - CEO
  - CXO (direct supervisor)
- Indirect Relationships
  - Enterprise Risk Committee
  - Regulatory & Compliance
  - Legal
  - Privacy



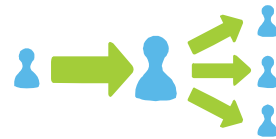
11

When you look at the org chart for the CISO, you might start to wonder how anything gets done. In many organizations, the CISO may report to the CIO for example, but to ensure that conflicts of interest don't get in the way, the CISO may also have a dotted line to the CEO. In addition, many organizations' Boards of Directors are becoming increasingly responsible for information security concerns, so the security program may also be required to report into the board's audit committee.

Then there are potentially numerous peer or reporting relationships with related functions such as Compliance, Legal, and Privacy. The CISO will also be required to be a part of or report regularly to the Enterprise Risk Committee for the organization. This gives the CISO a lot of power to escalate issues and get support from the highest levels of the organization, but beware. Use these avenues rarely and strategically. You may win the battle this way, but you may also lose the war.

## Security Liaisons

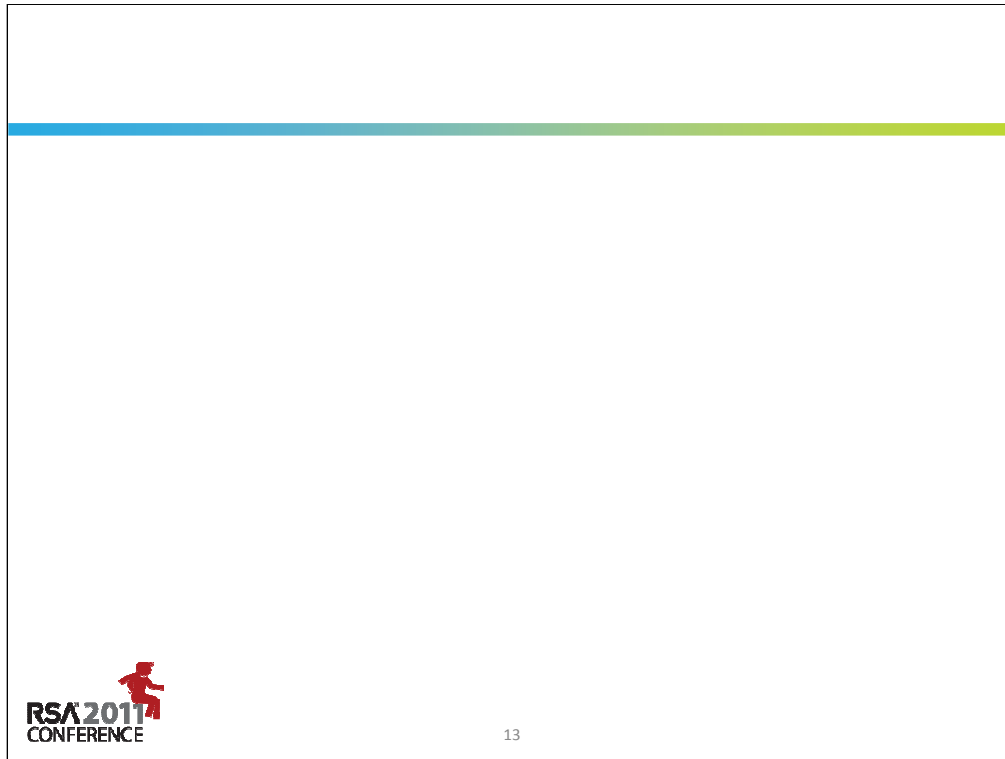
- Oversee risk assessments in their function
- Review & approve policy exceptions
- Ensure audit issues are resolved
- Delegate security tasks within their function
- Maintain inventory of information resources
- Represent function to security committees and review boards
- Principle contacts for security issues
- Educate function on security policies & initiatives



12

The theme for 2011 needs to be “doing more with less.” One tactic is to establish a role of a Security Liaison (also called a Security Maven or Information Security Lead) within other business units. This role is responsible for ensuring some aspects of the information security program in general, within their business unit. The scope of responsibilities will vary between organizations, but typically the role is responsible for and accountable for the oversight of security administration activities within their assigned functional areas, including some responsibility for security risk profiling of the information resources along with the resource owners. A train the trainer approach has become a common term in businesses who are looking for ways to save on the cost of education and training for their employees, and this is the same concept. The security team is responsible for training the liaisons and keeping them up to date with the latest developments and trends, and then can rely on them to carry that message to their own groups and translate into terms that will be more meaningful.

Those responsibilities above must be formalized as part of their personal performance objectives if you really want to see engagement from the liaisons. Essentially the security team can't be in every meeting and involved in every decision, so we need to enable a liaison from the various business units or functions to represent security interests on a daily basis. They are the key to executing a security program with limited staff.



Of course you can't expect this role to be successful without up front and on-going training and education. This includes the knowledge, skills, time, tools, and contacts to fulfill their role, but also the clear authority and support from the executive level so that this doesn't become a meaningless title. These liaisons can be a great way to expand the reach of the security function without additional headcount, so you should be able to free up some budget to ensure they have a steady stream of targeted training to keep them current. Also, you will want to keep a focus on keeping them informed about incidents, trends, changes in standards, and any new regulatory or legal requirements. Plan regular meetings and training sessions with them, and integrate them into your risk activities as much as possible.

Keep in mind that these volunteers will need to get the support from their own management to take on these responsibilities in addition to their current job function, so try to choose them carefully. You can often minimize the additional burden on these individuals by nominating individuals that already have close ties and complementary job roles to information security already. For example, someone from the legal staff may already be responsible for negotiating an ensuring the security clauses in contracts are sufficient, so that might be a logical choice, or someone in a business continuity or access provisioning role who works closely with the security team already.

## Outsourcing Security

- **Benefits**

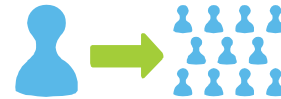
- Access to more specialized skills
- Deeper bench and more resources
- Awareness of trends across several organizations
- Can be a big cost savings
- Easier to provide 24x7 coverage
- Visibility across several organizations & industries

- **Challenges**

- Can you really trust your most sensitive function to a third-party?
- Need to perform due diligence
- Some functions lend themselves more to outsourcing than others

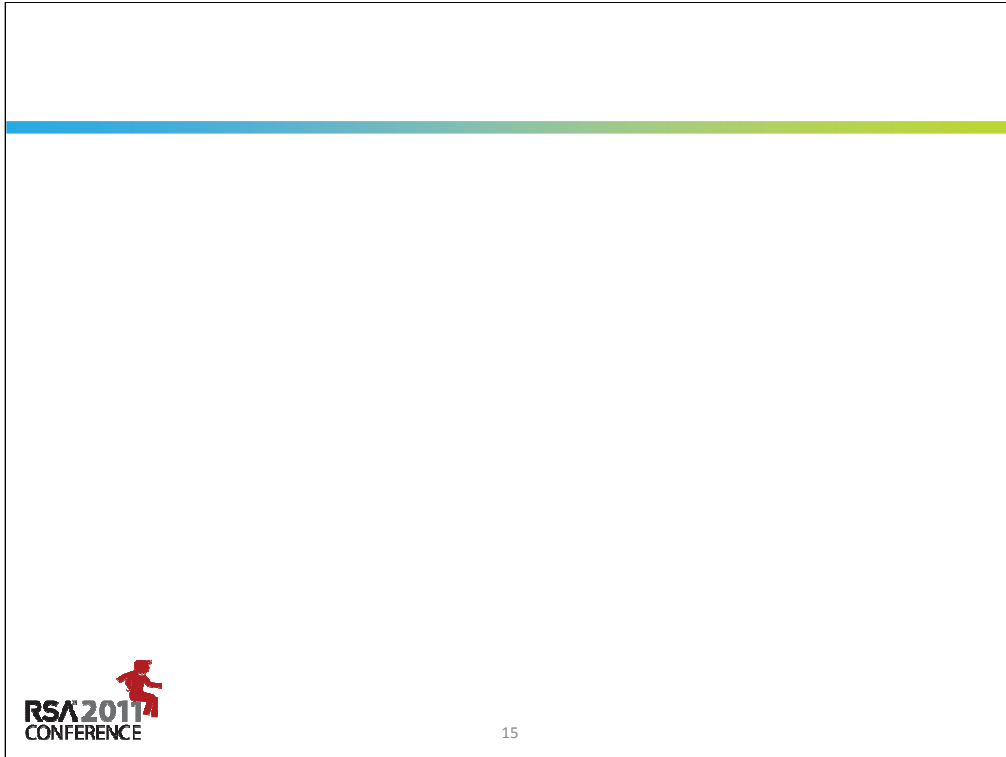


14



Ultimately for small and medium sized organizations, outsourcing parts of your security function to a third-party service may be more economical than building the capability in house. For larger organizations, it is usually more efficient to keep it in house. For one thing, they can provide 24x7 monitoring and triage services more easily and with a greater economy of scale than you could yourself. Plus they will be aware of trends across all the customers that they service, and that intelligence can be very valuable. Also, their staff will constantly exercising and expanding their skills, whereas internal staff is usually spread across several functions and may get rusty in some areas.

There are certainly many pros and cons to outsourcing any part of your security operations to a third-party provider. Obviously this requires a lot of upfront work to fully vet and analyze the possible service providers. If you stick with the large providers, than chances are that this due diligence has already been performed several times. Be sure to get references from clients in your same industry as a start. Even once you have selected a provider, you will need to perform regular re-assessments to ensure they stay in compliance with your policies.



You will always have to consider whether it is acceptable to rely on a third-party to service one of your most sensitive functions. It then becomes crucial for security managers to perform due diligence on the service provider and provide careful oversight. One function that lends itself very well to outsourcing is monitoring of security events from firewalls, IDS, IPS, and logging devices. Having a 24x7 tier 1 support for receiving the initial alerts and alarms, and filtering out any known false positives can be an essential service that can reduce your costs by not having to build out a full Security Operations Center (SOC) and staff a 24x7 support team. Hopefully this service provider can also provide intelligence about trends that they see across several of their clients.

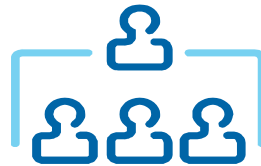
Training and awareness also lends itself to being outsourced to a third-party to develop content and training. Digital forensics is another good candidate. Other governance and oversight functions like risk management or architectural risk analysis may not be as easy to outsource.

## Convergence

- Risk Management
- Physical Security
- Information Security
- Business Continuity
  
- Compliance
- Privacy
- Legal
- Regulatory



16



When you think of security, all these functions should come to mind, but may not always in your day to day work. However, the term Information Assurance I think better describes the end goal for our field. It isn't just about the typical security protection responsibilities, the role of the CISO has to come to include major aspects of everything listed in the slide above as a core aspect of the program. Whether the program evolves to all report into a single Chief Security Officer, including information and physical security functions, or maybe under Risk Management, I think you will see in the next few years convergence of legal, compliance, and privacy functions. I believe that our current concept of information security will be absorbed into the risk management function, because it is far more focused on governance than enforcement.

## Apply Slide

---

- Organize your team by function (oversight vs. enforcement)
- Delegate out operational functions
- Establish clear reporting lines to the top
- Nominate security liaisons
- Analyze functions for outsourcing
- Integrate into risk management function

**END OF SECTION**



**RSACONFERENCE2011**