

# Defense-in-Policy begets Defense-in-Depth

Matthew Greenwell

# Defense-in-Policy begets Defense-in-Depth

*GIAC (GCED) Gold Certification*

Author: Matthew Greenwell, greenwellm@gmail.com
**Advisor: Chris Walker**
**Accepted: March 26, 2015**

Abstract

The majority of companies today focus solely on technical requirements for an information security program. When addressing the legendary AIC triad, companies focus on pulling controls from three categories: Administrative, Technical/Logical, and Physical/Environmental. Often, the Administrative category is overlooked, disregarded, and not given enough focus and attention from the business which can spell disaster for the security process as it provides the foundation and framework for the entire security program. One can no longer rely on technology alone to secure the perimeter, or for ad-hoc stove-pipe solutions to provide peace of mind. Organizations that invest more understanding and resources into their Administrative controls find security to be an enabling factor in their business instead of a process that is controlling and limiting to their business.

# 1. Introduction

Defense-in-depth is a commonly cited "best practices" strategy for achieving "Information Assurance". It is an approach to security that layers controls thus increasing security for the system as a whole (United States National Security Agency, n.d.). Security controls derive from three primary categories: administrative, technical/logical, and physical/environmental (Harris & Kumar, 2013, p. 28). By adapting their understanding and cogency of administrative controls, organizations can mature their security process. The information security market is flooded with technical solutions that fit into technical/logical control categories. As more businesses move to the Cloud, physical and environmental controls are relegated to third-parties. To achieve true Defense-in-Depth, businesses must further develop their Administrative controls and efforts. This enables the business to understand the value of security, and enables security to align with business strategy (Cano M., Ph.D., CFE, 2014, p. 51-55). This paper will examine the importance of administrative information security controls and the role they play in Defense-in-Depth strategies by discussing the maturity of security programs, discovery of security program foundations, frameworks, and process, enterprise security architecture, and the governance of information security strategies.

# 2. Mature Security Programs: Basics of Administration

## 2.1. What is Maturity in Security?

To better understand the relevancy of Administrative controls and their impact on security programs, it is important to understand how the industry defines maturity in security. Utilizing a system to establish maturity, "…helps organizations that can afford to invest only 20 percent achieve 80 percent of results (the 80/20 rule)," (Canal, 2008). Organizations can choose a baseline of security, per a particular information security management maturity standard, and use higher levels of a chosen maturity model as milestones to work toward. Maturity levels allow organizations to prioritize their security investments and measure improvement. To put it more delicately, "What you

Author Name, email@addressgreenwellm@gmail.com

can't measure, you can't manage, and what you can't manage, you can't improve." (Marr, 2006, p. 98).

There are many existing standards for measuring maturity in information security management. Some notable examples include: the Capability Maturity Model Integration (CMMI), NIST's Program Review for Information Security Management Assistance (PRISMA), ISM3, and ISO 14001. Diving in further to CMMI; the basis is to develop organized stages for an organization to follow to be able to evolve and mature. Here is an example of CMMI for a Security Program:

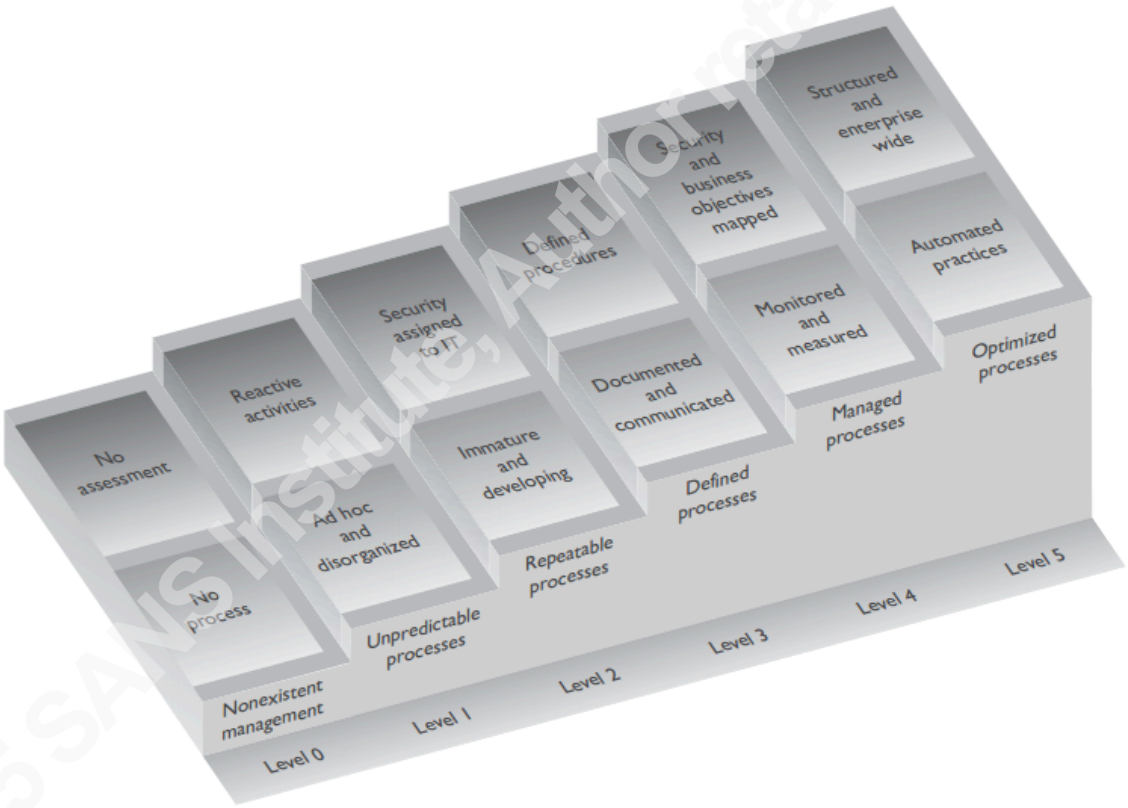


Figure 2-7. Capability Maturity Model for a security program. Reprinted from CISSP all-in-one exam guide, sixth edition (p. 62), Harris, S., & Kumar, P. V., 2013, New York, NY: McGraw-Hill. Copyright 2013 by McGraw-Hill Companies.

At a rudimentary level, immature security programs simply do not operate as a business process when organizations have not assessed themselves. They are reactive

and disorganized using ad-hoc solutions to address security concerns. Highly matured organizational security programs map security initiatives to business objectives and goals, they monitor and evaluate their processes, and they operate as an enterprise and automate their practices (Harris & Kumar, 2013, p. 62-63). No matter which standard is being utilized, integrating administrative controls is essential to maturing one's security program (National Institute of Standards and Technology, 2014).

## 2.2. AIC

Providing availability, integrity, confidentiality (AIC triad) is a key tenet of information security. Security revolves around the AIC triad; implementing controls and safeguards to provide protection around AIC, or measuring potential compromise to AIC via risk, threat, and vulnerability assessments (Stoneburner, 2001, p. 2-4). Maturity in security can only be obtained by balancing the security needs of an organization and aligning them with the principle of AIC. As aforementioned, maturity increases as organizations implement more administrative controls or "soft controls" that are more management-oriented (Harris & Kumar, 2013, p. 28). These controls provide support for the security program and establish the doctrine of the security process as it maps to the overall business strategy. Specific examples will be explored in section 2.4.

## 2.3. Managing Risk for the Organization

Security is, "the state of being protected or safe from harm…" or the absence of danger ("Security," n.d.). Discussed in the aforementioned section, protection of AIC can be achieved by measuring risks, threats, and vulnerabilities. This overall process can be identified as Information Risk Management (IRM), and risk management is a classic albeit critical Administrative control. Many organizations today—outside of the banking and financial industry—struggle to incorporate risk management processes. However, in a survey of Australian organizations taken by ISACA, one of the respondent's most important improvement initiatives was reported as alignment and integration of IT risk management and enterprise risk management (ERM). Developing and implementing an IT risk management framework was also ranked second overall for surveyed organizations. Further, when discussing risk management, or information risk management, it is important to note that it requires individuals to drive awareness and the

need across the business as a whole, rather than traditional focuses operating in silos (ISACA, 2014, p. 90-92).

The objective of Risk Management is not necessarily to eliminate all risk, but to discover, assess, treat, monitor and communicate risk in an organization. An example risk management process may look like the following:

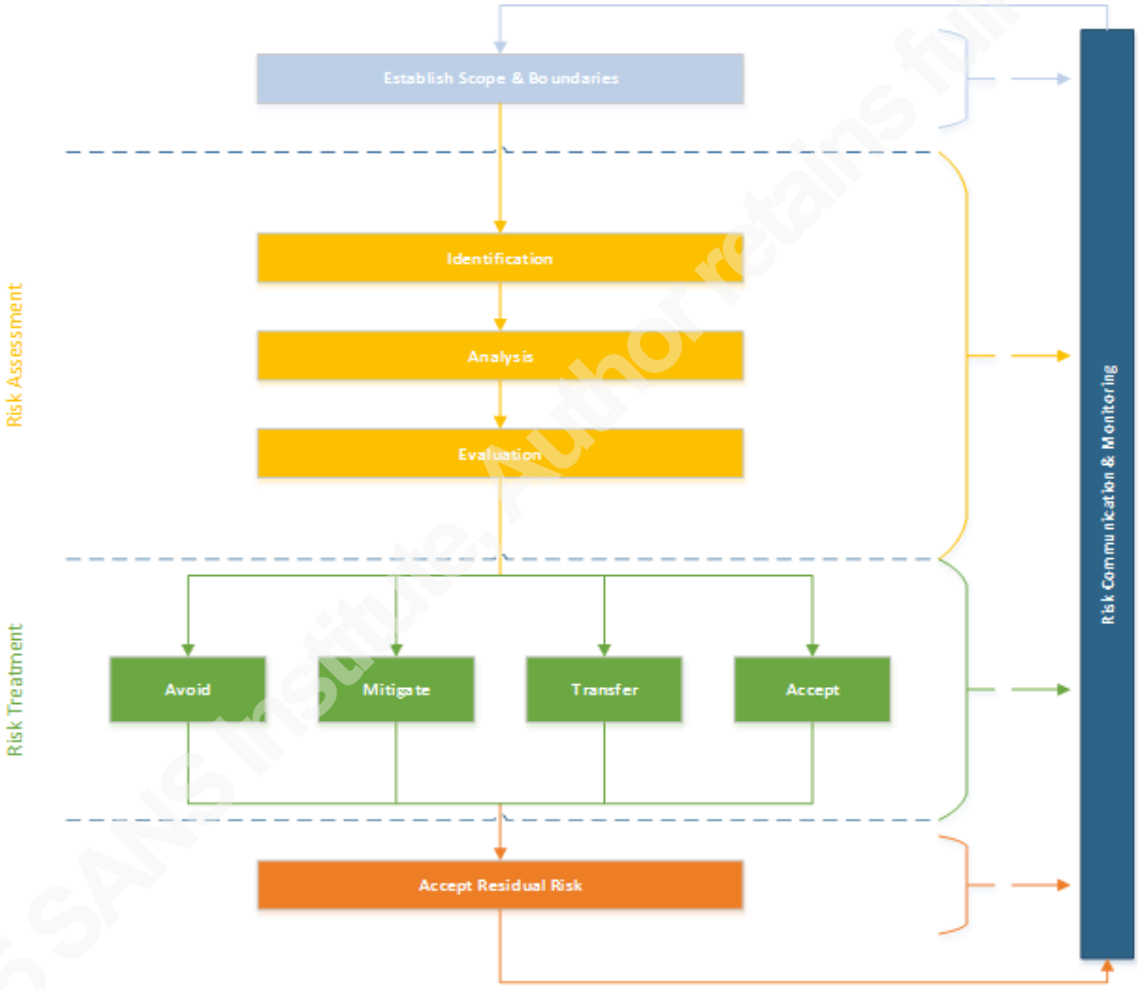


Exhibit 2.2. Risk Management Process. Reprinted from CISM Review Manual, 2014 edition (p. 95), ISACA, 2013, Rolling Meadows, IL: ISACA. Copyright 2013 by ISACA.

With risk management, organizations can empower internal audit programs to maintain or meet ever-growing compliance and regulatory requirements, reassure stakeholders, enhance business communications, and better support strategic and business planning all

the while promoting continuous improvement (ISACA, 2014, p. 89-94). An optimized risk management program can also lower the chances of a damaging security incident by prioritizing risk. This also allows organizations to save money by implementing more efficient controls and apposite levels of protection (James, 2012).

Organizations will face situations of risk where acceptance is necessary. All risk is eventually accepted, whether it be residual or inherent. Even transferring risk to an insurance company, the acting organization must still accept the risk responsibility and process with due care. After risk treatment, any residual risk must be accepted by the organization. If it cannot be, then more treatment is needed. In terms of risk appetite, some organizations may accept inherent risk because it is more costly to treat the risk than it is to accept it outright. The significance with the governance strategy in terms of risk management, is to continually monitor risk and the organizations changing appetite for risk (ISACA, 2014, p. 89-91).

## 2.4. Types of Controls

Information security controls are principally the weapons of information security; they are the protection and countermeasures offered to organizations through its security program. Controls come in three categories: Administrative, Technical/Logical, and Physical/Environmental. In relation to the control categories, there are additional types of controls that perform different functions: Deterrent, Preventive, Corrective, Recovery, Detective, and Compensating. Deterring controls are intended to dissuade a potential threat agent. Preventive controls are intended to avoid a security incident from happening. Corrective and recovery controls fix components after an incident has transpired and can help bring a situation back to normal operations. While detective and compensating controls help identify activities in an incident and provide alternative measures of a control (Harris & Kumar, 2013, p. 30-33).

### 2.4.1. Administrative Controls

Administrative controls can be referred to as “soft controls” due to their management focus. They are also considered actions that people take in the process of security (Northcutt, 2009). Commonly adopted administrative controls include:

- risk management,

- forensics/incident response,
- disaster recovery planning & business continuity planning,
- personnel training,
- policies (foundation), and
- baselines, guidelines, procedures, and standards (framework).

### 2.4.2. Technical/Logical Controls

Technical or logical controls use technology to control or limit access and usage of a system ("Red Hat Enterprise Linux 3: Security guide," n.d.). They can be ever-reaching in purview and include technologies such as:

- encryption,
- access control lists,
- file integrity monitoring software, and
- network authentication.

### 2.4.3. Physical/Environmental Controls

Physical and environmental controls are implemented to protect facility, personnel, and resources ("Red Hat Enterprise Linux 3: Security guide," n.d.). Many organizations employ standard physical and environmental controls such as the following:

- security guards,
- fences,
- mechanical door locks, and
- lighting.

By implementing and adopting administrative controls, organizations can enhance and enable their security programs to efficiently decide on additional controls in the technical/logical and physical/environmental controls. Establishing a risk management program enables organizations to prioritize their risks; an organization may discover that

their network perimeter is very weak and therefore invest in a next-generation firewall. Through personnel training, the next-generation firewall can be administered by trained and authorized staff. As a critical control, the next-generation firewall can be physically protected in a datacenter that imposes several access controls to be able to reach the device physically while also employing multi-factor logical access controls. Implementing controls together from various categories and of various types, enables an organization to perform Defense-in-Depth.

# 3. Foundation, Framework, and Process oh my!

## 3.1. Security is a Process

Information security management is first and foremost, a process. That is to say, it is "a series of actions that produce something or that lead to a particular result," as it pertains to information security ("Process," n.d.). As critical as the Administrative controls are that are designed as part of a security management process, naturally some administrative efforts are conducive to a well-designed and followed security process as well. Six sub-processes can be comprised to form a practical security management process; alertness, policy, strategy, compliance, monitoring, and access. One of the most important sub-processes is Policy. Policy ensures responsibility to organization members for securing business assets and it is used to decree standards in respect to security. Conversely, having a process for the assembly of security policy is essential to security management (Bayuk, n.d.).

It is vital for organizations to create formal, and dependable security processes that will bridge the gap between technology and business processes. It is also important for established security processes to remain updated (Therrien, 2013). In a 2014 report by RSA of security for business innovation taken from Global 1000 executives, archaic security processes' most challenging consequences included:

> Using technical terms for risk measurement makes advising business leaders difficult. Cumbersome manual methods for tracking risks are not business-friendly. Point in time piecemeal control assessments are no longer sufficient. The system for third-party security assessments and oversight needs fixing fast.

> Headway needs to be made towards meaningful collection and analysis of threat data," (Security for Business Innovation Council, RSA Security LLC, & EMC Corporation, 2013).

Recommendations for addressing the aforementioned problems are to align security more with the business and to prioritize focus and efforts. This can be achieved via administrative controls such as building a foundation and framework for the security program (Security for Business Innovation Council, RSA Security LLC, & EMC Corporation, 2013).

## 3.2. Building a Foundation and Framework

Policies provide the foundation for security. Typically, they are general statements provided by executive or senior management that defines the role security has within an organization. Policies can serve various functions such as regulatory, advisory, or informative. They set the stage, or foundation rather, for an organization's security program. Because the foundation of a security program can be crafted in ambiguity, more comprehensive efforts are needed to support it. This is where the framework comes into play; the baselines, guidelines, procedures, and standards. In order to be beneficial, these documents must be put into action and enforced. Training employees on their responsibilities and the role they play within the security program's foundation and framework, enables the workforce to support and adhere to senior management directives. Not only can training and enforcement of these concepts prevent negligence and liability of not practicing due care, it enables businesses to empower their individuals in helping them achieve business objectives and goals (Harris & Kumar, 2013, p. 101-108). In the "2014 US State of Cybercrime Survey," forty-nine (49) percent of respondents said vulnerability management policies and procedures helped deter potential criminals. Another forty-five (45) percent stated that policies and procedures regarding separation of duties helped their organization deter potential criminals (PricewaterhouseCoopers LLP, 2014). All of these are examples of administrative controls, and they allow organizations to integrate security into the business without a traditional stance of focusing solely on IT. This happens by bringing together the stakeholders and senior management to determine security's importance and focus within the business.

Author Name, email@addressgreenwellm@gmail.com

# 4. Enterprise Security Architecture

## 4.1. Defining the Enterprise

Not every organization functions as an enterprise. Many organizations attempt optimization and drive efficiency locally, at the department level. However, to be an enterprise, organizations must act as a single entity, rather than a set of collaborating departments. This allows improvements in competitiveness and services due to refining all parts of the organization all together in an intelligible way (Sherwood, Clark, & Lynas, 2005, p. xv). Aligning business processes and information security can be cumbersome. This is where an architectural approach to systems design is needed. There are various frameworks for systems and enterprise architectures, all of which aim to provide a holistic approach to security architecture while being an enabler for business (Sherwood, Clark, & Lynas, 2005, p. 29-30).

Enterprise architectures save businesses money by removing the confusion between business functionality and technical specifications. They allow business and technology groups to view the organization in ways that make sense to them (Harris & Kumar, 2013, p. 43-44). The enterprise security architecture is a subset of enterprise architecture that describes the structure and behavior of all components that make up a holistic information security program. The primary purpose in developing an enterprise security architecture is to align security efforts with business practices efficiently, and without great cost (Harris & Kumar, 2013, p. 49).

# 5. Governance

## 5.1. Aligning with Business

Alignment between management and security initiatives brings about governance. Governance in that there is a convergence between business management and information management. This allows senior management and stakeholders of organizations to best decide how security risks are dealt with and how the information security program should be designed and monitored (Calder & Watkins, 2006, p. 1-8). Governance functions establish and maintain clear accountability, authority and budget for information security management (Gartner, Inc., 2010).

Author Name, email@addressgreenwellm@gmail.com

## 5.2. Defining Success

Not all risks can even be treated by technical or logical controls. In the case of Occupational Fraud and Abuse, an effective governance approach to information security can have lasting impacts. In the "2014 Annual Report to the Nation on Occupational Fraud and Abuse by the Association of Certified Fraud Examiners," the findings were daunting. Several highlights include:

- Typical organizations lose five (5) percent of profits every year to fraud. Appropriated to the 2013 estimated Gross World Product, this equates to $3.7 trillion in losses due to fraud.
- Average loss triggered by fraud was $145,000; twenty-two (22) percent of cases involved losses over $1 million.
- Median duration of fraud activities lasted eighteen (18) months.
- Collusion increases fraud losses. Average loss in fraud perpetrated by a single individual was $80,000, however, as the number of participants amplified, losses rose exponentially.

Several recommendations were concluded in the report which included that many of the most effective anti-fraud controls—which implementation has shown to reduce fraud damage—are being overlooked by a majority proportion of organizations. These controls are administrative controls such as surprise audits, proactive data monitoring, separation of duties, and formal risk assessments (Association of Certified Fraud Examiners, 2014, p. 4-5). Generally, some elementary outcomes can be anticipated by developing an effective governance program cohesive with information security. This could mean a reduction of risks and number of potential business impacts, strategic conformity of security initiatives with business goals and objectives, and efficient utilization of security investments to support business strategy (Agile IT Governance, 2012).

Author Name, email@addressgreenwellm@gmail.com

## 6. Conclusion

Defense-in-Depth cannot be achieved without people or management-oriented controls. Documentation, risk management, and training are the very pillars that can allow organizations to operate free from danger. They provide the context and guidance needed to establish an information security program with purpose and direction. These can be, and in many cases are, required by law. Several regulations and laws are controls themselves because they inform the business.

Administrative controls allow organizations to better understand their existing state of security, as well as help to define their desired state. These controls allow organizations to efficiently spend resources on additional controls, such as those found in the technical/logical and physical/environmental categories. They provide the platform that all other controls stand on, and without them, security programs are doomed to fail.

However, failure to some degree must be accepted. Not all risks can be treated, and residual risk leaves room for failure of controls. One cannot prevent all data loss, or malware intrusions. As important as it is to define an organizations critical success factors, it is just as important to know how much failure is acceptable, i.e. risk appetite. Forming a holistic view of information security and how it aligns with the business—along with stakeholder input and senior management support—is the only way to structure and maintain a successful information security management system that protects the organization from danger.

Author Name, email@addressgreenwellm@gmail.com

# References

Agile IT Governance. (2012, November). 5 Benefits of proper IT security governance. Retrieved from http://agileitgovernance.com/2012/11/08/5-benefits-of-proper-it-security-governance/

Association of Certified Fraud Examiners. (2014). *Report to the Nations on occupational fraud and abuse*. Retrieved from http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

Bayuk, J. L. (n.d.). Security through process management. Retrieved from http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper015/bayuk.pdf

Calder, A., & Watkins, S. (2006). *International IT governance: An executive guide to ISO 17799/ISO 27001*.

Canal, V. A. (2008). Usefulness of an information security management maturity model. *Information Systems Control Journal*, *2*. Retrieved from http://www.isaca.org/Journal/archives/2008/Volume-2/Documents/jpdf0802-usefulness-of-an-info.pdf

Cano M., Ph.D, CFE, J. J. (2014). The information security function: Current and emerging pressures from information insecurity. *ISACA Journal*, 51-55. Retrieved from http://www.isaca.org/Journal/archives/2014/Volume-6/Documents/Journal-vol-6-2014.pdf

Gartner, Inc. (2010). *Best practices: The information security organization, 2010*(G00175047).

Harris, S., & Kumar, P. V. (2013). *CISSP all-in-one exam guide, sixth edition* (6th ed.). New York, NY: McGraw-Hill.

Author Name, email@addressgreenwellm@gmail.com

ISACA. (2014). *CISM Review Manual* (2014 ed.). Rolling Meadows, IL: Author.

James, D. (2012, February). Seven solid benefits of information risk management. Retrieved from http://www.ascentor.co.uk/2012/02/seven-solid-benefits-of-information-risk-management/

Marr, B. (2006). *Strategic performance management: Leveraging and measuring your intangible value drivers*.

National Institute of Standards and Technology. (2014, April). Security maturity levels. Retrieved from http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html

Northcutt, S. (2009). Security controls. Retrieved from http://www.sans.edu/research/security-laboratory/article/security-controls

PricewaterhouseCoopers LLP. (2014). *US cybercrime: Rising risks, reduced readiness; Key findings from the 2014 US State of Cybercrime Survey*. Retrieved from http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Process. (n.d.). In *Dictionary and Thesaurus | Merriam-Webster*. Retrieved from http://www.merriam-webster.com/dictionary/process

Red Hat Enterprise Linux 3: Security guide. (n.d.). Retrieved from https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/s1-sgs-ov-controls.html

Security for Business Innovation Council, RSA Security LLC, & EMC Corporation. (2013). *Transforming information security: Future-proofing processes*. Retrieved

Author Name, email@addressgreenwellm@gmail.com

from http://www.emc.com/collateral/white-papers/h12622-rsa-future-proofing-processes.pdf

Security. (n.d.). In *Dictionary and Thesaurus | Merriam-Webster*. Retrieved from http://www.merriam-webster.com/dictionary/security

Sherwood, J., Clark, A., & Lynas, D. (2005). Enterprise security architecture: A business-driven approach. Boca Raton, FL: CRC Press.

Stoneburner, G. (2001). *Underlying technical models for information technology security*. Retrieved from National Institute of Standards and Technology website: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

Therrien, L. (2013, December 10). Five ways to future-proof information security processes [Web log post]. Retrieved from https://blogs.rsa.com/five-ways-future-proof-information-security-processes/

United States National Security Agency. (n.d.). Defense in Depth. Retrieved from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

Author Name, email@addressgreenwellm@gmail.com

Last Updated: September 18th, 2019

# Upcoming SANS Training

**Click here to view a list of all SANS Courses**

| | | | |
|---|---|---|---|
| SANS San Francisco Fall 2019 | San Francisco, CAUS | Sep 23, 2019 - Sep 28, 2019 | Live Event |
| SANS Dallas Fall 2019 | Dallas, TXUS | Sep 23, 2019 - Sep 28, 2019 | Live Event |
| SANS London September 2019 | London, GB | Sep 23, 2019 - Sep 28, 2019 | Live Event |
| SANS Kuwait September 2019 | Salmiya, KW | Sep 28, 2019 - Oct 03, 2019 | Live Event |
| SANS Tokyo Autumn 2019 | Tokyo, JP | Sep 30, 2019 - Oct 12, 2019 | Live Event |
| SANS Cardiff September 2019 | Cardiff, GB | Sep 30, 2019 - Oct 05, 2019 | Live Event |
| SANS Northern VA Fall- Reston 2019 | Reston, VAUS | Sep 30, 2019 - Oct 05, 2019 | Live Event |
| SANS DFIR Europe Summit & Training 2019 - Prague Edition | Prague, CZ | Sep 30, 2019 - Oct 06, 2019 | Live Event |
| Threat Hunting & Incident Response Summit & Training 2019 | New Orleans, LAUS | Sep 30, 2019 - Oct 07, 2019 | Live Event |
| SANS Riyadh October 2019 | Riyadh, SA | Oct 05, 2019 - Oct 10, 2019 | Live Event |
| SANS Baltimore Fall 2019 | Baltimore, MDUS | Oct 07, 2019 - Oct 12, 2019 | Live Event |
| SANS October Singapore 2019 | Singapore, SG | Oct 07, 2019 - Oct 26, 2019 | Live Event |
| SANS Lisbon October 2019 | Lisbon, PT | Oct 07, 2019 - Oct 12, 2019 | Live Event |
| SANS San Diego 2019 | San Diego, CAUS | Oct 07, 2019 - Oct 12, 2019 | Live Event |
| SIEM Summit & Training 2019 | Chicago, ILUS | Oct 07, 2019 - Oct 14, 2019 | Live Event |
| SANS Doha October 2019 | Doha, QA | Oct 12, 2019 - Oct 17, 2019 | Live Event |
| SANS Seattle Fall 2019 | Seattle, WAUS | Oct 14, 2019 - Oct 19, 2019 | Live Event |
| SANS SEC504 Madrid October 2019 (in Spanish) | Madrid, ES | Oct 14, 2019 - Oct 19, 2019 | Live Event |
| SANS Denver 2019 | Denver, COUS | Oct 14, 2019 - Oct 19, 2019 | Live Event |
| SANS London October 2019 | London, GB | Oct 14, 2019 - Oct 19, 2019 | Live Event |
| SANS Cairo October 2019 | Cairo, EG | Oct 19, 2019 - Oct 24, 2019 | Live Event |
| SANS Santa Monica 2019 | Santa Monica, CAUS | Oct 21, 2019 - Oct 26, 2019 | Live Event |
| Purple Team Summit & Training 2019 | Las Colinas, TXUS | Oct 21, 2019 - Oct 28, 2019 | Live Event |
| SANS Training at Wild West Hackin Fest | Deadwood, SDUS | Oct 22, 2019 - Oct 23, 2019 | Live Event |
| SANS Orlando 2019 | Orlando, FLUS | Oct 28, 2019 - Nov 02, 2019 | Live Event |
| SANS Houston 2019 | Houston, TXUS | Oct 28, 2019 - Nov 02, 2019 | Live Event |
| SANS Amsterdam October 2019 | Amsterdam, NL | Oct 28, 2019 - Nov 02, 2019 | Live Event |
| SANS DFIRCON 2019 | Coral Gables, FLUS | Nov 04, 2019 - Nov 09, 2019 | Live Event |
| Cloud & DevOps Security Summit & Training 2019 | Denver, COUS | Nov 04, 2019 - Nov 11, 2019 | Live Event |
| SANS Paris November 2019 | Paris, FR | Nov 04, 2019 - Nov 09, 2019 | Live Event |
| SANS Sydney 2019 | Sydney, AU | Nov 04, 2019 - Nov 23, 2019 | Live Event |
| SANS Mumbai 2019 | Mumbai, IN | Nov 04, 2019 - Nov 09, 2019 | Live Event |
| SANS Bahrain September 2019 | OnlineBH | Sep 21, 2019 - Sep 26, 2019 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |