CISSP: The Domains

Certification Foundations

INFO SEC INSTITUTE

INTENSE SCHOOL

Ken Magee

CISSP: The Domains

InfoSec Institute – Certification Foundations

INFO
SEC
INSTITUTE

Table of Contents

INTRODUCTION

(ISC)²'s CISSP Exam covers ten domains which are:

- Access Control
- Application Development Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security Governance and Risk Management
- Legal regulations, investigations, and compliance
- Operations Security
- Physical and Environmental Security
- Security Architecture and Design
- Telecommunications and Network Security

Over the course of the this eBook, we'll take a look at each one of the domains; give you some insight into what (ISC)² is looking for in that area; give you some supplemental reading material; and by the time we're done, you should have the foundation of the information you'll need to pass the CISSP exam as well as to succeed in your security professional career. **You will go into your CISSP boot camp well-prepared and come out with your certification!**

I will say this, one of the ways that you can ensure your preparation for the CISSP exam is by taking the InfoSec CISSP Boot Camp course. As far as reading material is concerned, everyone should have their own personal copy of the CISSP CBK 2nd Edition from (ISC)². All quoted material in this guide is from the "Official (ISC)² Guide to the CISSP® CBK Third Edition."

A QUICK NOTE ON FORMATTING:

ISC² published the 3rd edition of their CISSP CBK in late 2012. I ordered my copy in December 2012 and said, "So what's new?" Each of the 10 domains is a chapter, and each chapters starts off with a "what's new" section. So if you've studied up in the past or are part way through previous material, it will be beneficial to at least read through the beginnings of each of the chapters.

DOMAIN 1:

ACCESS CONTROL

> *"Instructor used a good blend of instruction, humor and testing. I liked how he took his time (and made us take our time) on review questions so that everyone had a chance to ask questions and understand why something was right or wrong. Great experience!"*
>
> **Betsy Powlen**
> **Logis-Tech**

WHAT'S NEW IN ACCESS CONTROL?

I started going through the Access Control domain and these are some of the changes that I found:

- For "Personnel Security, Evaluation, and Clearances" and additional source of information for staff verification has been added. "…An online search of publicly available information on social media sites…"
- A whole section has been added for "Session Management" and includes two major areas:
  1) Desktop Sessions and 2) Logical Sessions. The Desktop Session section had several sub-sections including:
  - Screensavers
  - Timeouts and Automatic Logouts
  - Session/Logon Limitation
  - Schedule Limitations

An interesting addition as a key point to remember about Kerberos was added, it reads, "...Kerberos processes are extremely time sensitive and often require the use of Network Time Protocol (NTP) Daemons to ensure times are synchronized. Failure to maintain a synchronized time infrastructure will lead to authentication failures. This can be an attractive vector for a DOS attack…"

There's a new section on Security Information and Event Management. It goes into some detail with respect to log management and something that I've been saying for several years and that is "near real time" management of security information.

Spyware has been expanded to identify and discuss "Malvertisements" and "Malnets."

Threat Modeling has gotten its own section, including some specific steps for organizations to take as an approach. Those steps include:

- Define the Scope and Objectives
- Understanding or Modeling the System
- Development of Threats
- Development of Vulnerabilities
- Determining Impacts and Risk
- Develop a Mitigation Plan

We use to see this strategy as part of Business Impact Analysis and Risk Assessment but it has been moved to Access Control. That is also true for "Asset Valuation" which has been moved to Access Control and includes:

- Hardware
- Software
- Integration
- Opportunity Costs
- Regulatory Exposure
- Information Replacement
- Reputational Exposure

Also included in this section are the calculations for SLE and ALE which we use to find in the Risk domain.

The last two major areas, which received additional coverage includes, "Access Review and Audit" and "Identity and Access Provisioning Lifecycle."

Of course along with any change you get re-sequencing, font size change, bolded emphasis, and the occasional colorful metaphor. All-in-all, I'm pleased with the revisions to this domain and I look forward to the other nine.

InfoSec Institute is in the process of updating their CISSP curriculum and where appropriate will include coverage of any new material which is included in the new CISSP CBK.

An Overview

There are several areas within access control which are covered on the CISSP exam. Those areas include IAAA (Identification, Authentication, Authorization and Accountability), access control techniques & technologies, administration, control methods, control types, accountability, control practices, monitoring and threats to access control. This article deals specifically with the role based access control model (RBAC). RBAC's usage is widespread across all industries; allows organizations to address securing access control; and RBAC is receiving an increased interest from (ISC)² in terms of questioning the knowledge the CISSP candidate has relative to RBAC.

Role based access control presents a unique opportunity for organizations to address the principle of Least Privilege, which is giving an individual only the access they need to do their job since the access is tied to their job. In a Windows or UNIX/Linux environment this is typically done by developing Groups. The Group has individual file permissions and each individual is then assigned as a member of that Group. At the same time however, organizations need to periodically review the role definitions and have a formal process in place to modify roles and to test for segregation of duties. Otherwise without monitoring and review there is a possibility that Role Creep will develop where an individual, say as an Accounts Payable clerk who had membership in the group which could add vendors is transferred to another job within AP and now is responsible for entering invoices. Without review, that individual could now have both roles and could add vendors as well as enter invoices for the same vendors. Not a good segregation of duties.

David Ferraiolo and Rick Kuhn in their book Role Based Access Control proposed the RBAC model based on the premise that it reduces the overall cost of maintaining secure access control.

That model has since been adopted as an ANSI/INCITS standard. ANSI/INCITS 359-2004 standard.

Role based access control is not a mandatory access control (MAC) nor is it a discretionary access control (DAC). (MAC) refers to a type of access control by which the operating system controls access to the information. This is typically done by the OS system administrator when the OS is configured, for example, which programs need to have administrative privileges to run. DAC is an access control similar to the traditional Unix system of users, groups, and read-write-execute permissions where the owner controls who has access to the information. With RBAC, access is assigned to users based on the job they have, or the role they play in the organization. For example, when a person working as an Accounts Payable Clerk is promoted to an Accounts Receivable Clerk their access to the Accounts Payable system is changed. It is not done screen by screen, file by file or drive by drive, but as a group based on their new job, or role. Some accesses may be eliminated but others are likely granted.

When that individual is terminated or transferred, the security administrator simply removes the assigned role, thus removing all of that individual's access for the previous role. This also answers the question of least privilege, since the assignment is role-based and not individual based. This might appear to be more work rather than less work. This is true for the initial setup. However, once the system/data owners have identified the different roles then it is a matter of assigning different roles rather than individual file or data access.

The National Institute of Standards and Testing (NIST) administers RBAC. If you are interested in reading further about RBAC, there is news, case studies, and help in implementing the standard on their site at: http://csrc.nist.gov/groups/SNS/rbac/

NIST is currently investigating revising the RBAC standard. To become involved in developing this important standard, check out: http://csrc.nist.gov/groups/SNS/rbac/rbac-standard-revision.html

Domain 2:

Software Development Security

"I would certainly recommend to my co-workers… truly outstanding!!"

Douglas Jones
Defense Threat Reduction Agency

What's new in Applications Security (Now Software Development Security)?

So what's new in Software Development Security, besides the apparent name change from Application Security?

I started going through this domain and other than some re-sequencing, only found two minor changes.

- Web Application Threats and Protection section, got an extra paragraph which identifies the Open Web Application Security Project (OWASP) and their guides for web app development.
- The Certification and Accreditation section, received an extra paragraph, outlining several reasons why a private organization may choose to undergo a formal authorization process.

All-in-all it appears to me that the biggest change, apart from the name change, was some re-sequencing.

An Overview

Application development security requires an awareness of how different environments demand different security. For example, the security for running a mainframe application that is not accessible by anything except the mainframe would be considerably different than the security for a web based application that anyone on the internet has access to. Other important questions that impact the application's security include: How complex an application is it? What are the data types, formats, and lengths? What are the failure states? Which database management system is being used? All of these questions will impact the application's security.

I would be remiss if I didn't mention system development life cycle, or SDLC. You will need to remember all those phases from feasibility through operations. As well as the ideas of prototyping, rapid application development (RAD), joint application development (JAD), and bad application development (BAD). Just kidding on the last one. However, if you run short of time there's always Agile and CASE to speed up the process.

(ISC)^2 is showing a lot of interest in three areas within Application Development Security: Web Security, Mobile Code and Patch Management. Let's take a closer look at each.

Let's examine Web Security first. A lot of the application code being developed today revolves around the internet. The InfoSec Institute has an excellent course in Web Application Penetration Testing, during which you will learn not only how to attack but also how to defend your Web Application. Web Application Security includes DoS (Denial-of-service) attacks, web application firewalls IDSs and IPSs. OWASP and SANS both, list Web Application vulnerabilities in the top 10. As is the case with any application development effort, you need to remember three things: 1) Always validate your input, this is especially critical in web applications development when we look at vulnerabilities like cross-site scripting and SQL injection, 2) Always validate the data during processing, and finally 3) always validate the output data. Also in web application development how you manage your session and whether you choose to use cookies or not needs to be carefully considered and the risks weighed against the business needs.

Any discussion of Mobile code should include subjects like Java Applets, ActiveX Controls, Malware, Antivirus Software, Spam Detection software and others. All of these represent potential weaknesses in your application security, whether it's choosing to include JavaScript or Python script in your development of applets or ActiveX controls for your application or whether it's deciding if you want to make your code truly mobile with an iPad version. The same as with web application development, mobile code development needs to have a vulnerability scan ran against the code before it's put into production.

And finally, Patch Management is an area that is relatively easy to address, but is often overlooked. Every organization should have a patch management policy and all systems, including systems under development should be "patched." Let's face it, there are a lot of IT folks out there as well as some non-IT folks who are doing system development. And that's in all areas; application, operating system, database, network communication, etc.

In application development security it is crucial that you ensure that the operating system you're going to be running on in production is current and patched. It's equally crucial that you make sure the database your application is going to be using is current and patched. Known vulnerabilities have been identified and vendors have already patched them. So give your application the best vulnerability security available and that is a system that is patched which has a program behind it to keep it patched. And yes, I know every time the OS or DB is patched you will have to retest your application. However, that's part of application development security.

Speaking of databases, just a few words that (ISC)^2 keeps putting into the exam. Look these up for your own reference:

- ANN (Artificial Neural Networks)
- Referential Integrity
- Data Normalization
- Data De-normalization
- Data Warehouse

DOMAIN 3:

BUSINESS CONTINUITY & DISASTER RECOVERY

> *"The instructor taught in such a way were everyone could understand the subject. He also went as far as demonstrating real situations to impact what was taught."*
>
> **Richard Kesterson**
> **US Navy**

WHAT'S NEW?

One thing I noticed different about this domain is there are documented footnotes for most of the references, e.g.NFPA1600[3] now has 3. http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf

Here are the things that I found different in Business Continuity and Disaster Recovery Planning.

- The section on "Coordination with Public Authorities" references BS 25999 stage 2 being replaced by ISO 22301 in 2012. ISO 22301:2012 was actually published May 15, 2012
- The section on "Regulations for US Financial Institutions" has been updated with new laws to include:
    - US Financial Integrity Regulatory Authority (FINRA) Rule 4370, The Australian Prudential Standard CPS232, Monetary Authority of Singapore,
    - Standard for Business Continuity/Disaster Recovery Service Providers (SS507), and
    - HIPAA

- In the section on "Recovery Site Strategies" several new sections have been added to include:
    - Mobile Sites
    - Processing Agreements, which include:
        - Reciprocal agreements
        - Outsourcing
    - Multiple Processing Sites
- A section was added entitled "Assessment" which states that events need to be categorized as"
    - Non-Incident
    - Incident
    - Severe Incident
- The Disaster Recovery Exercise Report sample has the title changed from 2008 to 2013; everything else in the sample is the same.
- In the section on "Transitioning from Project to Program" there is a bulleted list in the paragraph which starts out with "The EMO management team." The 9th bullet point is actually a new paragraph, but somehow it got a bullet instead. That's the one that reads "Each of these groups has specific responsibilities in the event of an emergency, including:"

As always, InfoSec is updating the courseware to reflect this new material and re-sequencing of the Business Conti-unity and Disaster Recovery Planning domain.

AN OVERVIEW

You only have to turn on the TV and watch some of the footage of the destruction caused by the tsunami in Japan to realize the importance of business continuity and disaster recovery planning or think back to the September 11 attacks and remember the destruction in New York City to realize the importance of business continuity and disaster recovery planning.

The CISSP exam as well as the certification exams from the Disaster Recovery Institute International (ABCP-Associate Business Continuity Professional, CBCP-Certified Business Continuity Professional, and MBCP-Master Business Continuity Professional) all focus on the same issues, namely continuing business in the event of a disaster.

There are several definitions that you need to know for this domain:

BCP (Business Continuity Plan) – the overall organizational plan for "how-to" continue business.

COOP (Continuity of Operations Plan) – the plan for continuing to do business until the IT infrastructure can be restored.

DRP (Disaster Recovery Plan) – the plan for recovering from an IT disaster and having the IT infrastructure back in operation.

BRP (Business Resumption Plan) – the plan to move from the disaster recovery site back to your business environment or back to normal operations.

MTBF (Mean Time Between Failures) – a time determination for how long a piece of IT infrastructure will continue to work before it fails.

MTTR (Mean Time to Repair) – a time determination for how long it will take to get a piece of hardware/software repaired and back on-line.

RPO (Recovery Point Objective) – is the organization's definition of acceptable data loss.

RTO (Recovery Time Objective) – is the organization's definition of the acceptable amount of time an IT system can be off-line.

Let's begin this domain by enumerating some tasks that need to be performed in order to be successful at business continuity and disaster recovery. The first thing an organization needs to do is to complete a Business Impact Analysis (BIA). That BIA will identify all of the business functions, which then need to be evaluated to determine which ones are critical to the business and which ones aren't. The BIA also includes which IT assets are required to support the business function as well as which supporting business functions are required. So in addition to the BIA, the organization needs to have an accurate IT asset inventory to support those functions. Once those two pieces are complete, but still in the BIA process, the owner of the business function needs to define the Recovery Point Objective and the Recovery Time Objective. The RPO will help IT determine what backup strategy will be required. For example, let's say the owner of the business function states they can afford to lose up to one day's worth of entered data. Your choice in this case might be to have weekly full backups and daily incremental or differential backups. You will need to understand the following terms related to backups: Full, Incremental, Differential, Electronic Vaulting, Remote Journaling, Database Shadowing and High Availability. Pay particular attention to how many tapes would be required to restore a system if it crashed mid-week and you were doing Full and Daily Incremental vs. Full and Daily Differential.

Now that the owner of the business function has completed the BIA there will likely need to be some negotiation with IT. For example, the BIA has an RTO of four hours and IT knows that it takes eight hours to rebuild the server. With a little give and take on both sides — and there are always options — in this case it might make sense to change the RTO to eight hours or to purchase a second server and implement HA (High Availability) clustering.

The next thing we want to look at is the COOP. The COOP is where the owner of the business function will define how they're going to continue to do business while IT is restoring the systems that crashed. Pay particular attention to (HINT) documented procedures for manual processes. The COOP will also include things like succession planning, contacts with external authorities, and contact lists. Remember in a disaster scenario, people act differently so when you put someone's phone number down, don't put the office number only, because the office is no longer there. Put an alternate phone number down and remember to put the area code and/or country code because people will dial what they see and if you have people in different area codes, they need to know the full phone number.

Just a quick sidebar on preventive measures like surge protectors, UPSs, backup generators, dual but separate power feeds, dual but separate ISP connections. OK, enough said, you get the picture. If you have a data center or just a server room, you need to consider all of those things which go into supporting the infrastructure to "PREVENT" interruptions from occurring.

Now when you talk about your Disaster Recovery Plan (DRP) you need to know the different types of recovery sites or options; namely reciprocal agreement, cold site, warm site, hot site, redundant site and mobile sites. Two things come to mind, the first is cost and the second is availability. Obviously it is more expensive to have a mirror image redundant site and it is debatable as to whether a reciprocal agreement will actually provide the facilities you need in the event of a disaster. One thing to consider, particularly in light of 9/11 and the recent tsunami, is how many businesses are using your same backup site and what happens if that backup site can't support a major disaster? What's your backup plan? Where's your secondary site? And last, but not least, are your backups; tapes or whatever; protected from the same disaster. In other words are they stored a reasonable distance away from your business such that the disaster will not affect the backups.

Finally, but probably most important, is the testing of the plans, all of them, BCP, COOP, DRP, and BRP. You need to know the different types of testing, such as, checklist, structured walkthrough/tabletops, simulation, parallel processing, and full business interruption testing. And of course, to go along with all this testing don't forget to train your recovery team members.

Now as a parting note there are a few documents and websites you need to become familiar with:

Documents:

- NIST SP 800-34
- ISO/IEC-27031
- BS25999

Websites:

- https://www.drii.org/
- http://www.thebci.org/

DOMAIN 4:
CRYPTOGRAPHY

"Awesome!!! The materials in the course were great and the instructor's way of teaching made the information very easy to understand. I definitely recommend."

Branden Alexander
Fort Meade

U.S.ARMY

WHAT'S NEW?

Here are the things that I found different in Cryptography.

Preceding the section on "Issues Surrounding Cryptography" they've added a section on "The Cryptographic Lifecycle" and a section on "Algorithm/Protocol Governance."

They added a single page on "**Non-Repudiation,"** no make that 2/3 of a page, sort of as an after-thought to Digital Signatures. The bulk of this short page is the definition from NIST SP 800-57. The rest is 7 lines of how to accomplish non-repudiation which is almost the same as the last paragraph of the section on digital signatures.

One typo of note – a known plaintext attack is listed as "**Know plaintext."**

Checksums got dropped from 2nd Edition, or at least I couldn't find it in 3rd Edition.

As always, InfoSec Institute has updated courseware to reflect this new re-sequencing of the Cryptography domain.

AN OVERVIEW

There are books upon books about cryptography and this article will not attempt to regurgitate all of the historical background about the subject. However, there are some specific definitions and concepts that you need to understand in order to successfully navigate the CISSP exam and, for that matter, to be successful in your job.

- First let's take a look at some definitions:
- Plaintext — That's what you're reading now, plain text.
- Cipher text — That's encrypted text, plain and simple.
- Encryption — That's taking a plain text message and converting it to cipher text.
- Decryption — That's taking an encrypted text, or cipher text, and converting it back to plaintext.
- Cryptology — Is the science of securing data.
- Cryptography — Is the process of converting plaintext to cipher text a.k.a. encryption.
- Cryptanalysis — Is the science of breaking the code or decrypting the data.
- Cryptology — Encompasses both cryptography and cryptanalysis.
- Cipher — Is an algorithm for performing encryption or decryption.
- Algorithm — Is a set of rules that precisely defines a sequence of operations.

We'll cover more definitions later. Now let's look at some math. You need to be familiar with modular math, which is basically what the remainder is after division. As an example, 7 Mod 3 is what? 1 of course. That's because 3 goes into 7 twice with a remainder of 1. I've seen that exact question on an exam. Even something as simple as telling time is modular math. Think about it, two hours past 11 PM is 1 (2+11 = 13, 13/12 = 1 with a remainder of 1) a remainder of 1 so it must be 1 AM.

Before I forget, let's define Steganography as the hiding of things in things. For a neat way of learning about Steganography, download version 4 of S-Tools from Finland from http://soft.softoogle.com/ap/s-tools-download-126.shtml. Download it and play around with it. For those of you interested in a quick tutorial on S-Tools, you can read this article.

When we're talking about ciphers, there's really two basic types: substitution and transposition. Substitution is simply substituting one character for another, e.g. in the word FOOD we substitute B for F, E for O, and T for D and instead of the word FOOD, we now have BEET.

In transposition, we simply rearrange the letters, e.g. in the word DRAB we transpose the D and B and the resulting word is BRAD.

When we talk about algorithms, we have to talk about symmetric and asymmetric. I know I said I wouldn't talk about history, but you have to remember a little history of algorithms here, at least for the exam. Remember that symmetric is ONE key, also known as a secret key. Whereas, asymmetric is two keys, or a pair of keys, known popularly as public/private key pair. Now this may be obvious, but who knows your public key? Right, everyone. And who knows your private key? Only you, correct.

So here's an important concept: When you see "non-repudiation" that means you can't deny something is yours. If you encrypt something with your private key and you're the only one with your private key, then you can't deny something is yours. Anyone can decrypt the message but everyone knows it came from you.

Let's take it a step further, on a second pass of encryption (encrypted a second time — HINT: that's a test question) you use the receiver's public key. Who can decrypt the message now? Only the receiver, since they're the only one with the matching private key, thus ensuring confidentiality.

So how do I ensure integrity? I take the message and digitally sign it. I generate a SHA-1 hash of the plaintext message and encrypt the hash with my private key. You receive the message, run your own SHA-1 hash, decrypt the attached hash and compare the two, and if they are the same you know the message hasn't been changed.

There's a lot of other things you need to read up on using Google or a reliable Wiki. Things such as block ciphers, stream ciphers, DES and Triple-DES will come up. While you're looking at DES, also find the definitions for electronic code book (ECB), cipher block chaining (CBC), cipher feedback (CFB), output feedback (OFB) and counter mode (CTR). You should also know the differences in encryption strength between DES and Triple-DES. I've also seen a question on the exam that asks about the difference between DES and Double-DES. Now there's an interesting Google search.

So, which systems are symmetric?

- Data Encryption Standard (DES)
- Triple-DES
- The Advanced Encryption Standard (AES)

- International Data Encryption Algorithm (IDEA)
- Blowfish
- RC4
- RC5
- RC6
- And which systems are Asymmetric?
- The Diffie-Hellman Algorithm
- RSA
- El Gamal
- Elliptic Curve Cryptosystems (ECC)
- Knapsack

You will also need to read up on Public-Key Infrastructure (PKI) and make sure you understand the roles that Certificate Authorities (CA), and Registration Authority (RA) have. As well as what the PKI steps are.

When we talk about e-mail standards, you need to understand MIME and S/MIME as well as having a fairly good understanding of PGP. Like I said in the beginning, I'm not going into a lot of detail, there're books out there for that.

When we talk about internet security, there's more than just basics. Remember, if you're going to be using the internet for communications, use VPN. You also need to understand AH and ESP.

There are many different attacks against encrypted data. These are the ones you'll need to understand for the exam.

1. Cipher-Only Attacks
2. Known-Plaintext Attacks
3. Chosen-Plaintext Attacks
4. Chosen-Cipher text Attacks

Remember that cryptography covers a huge area of knowledge and has been around since the time of Caesar. Get a good book on the subject, find a soft comfortable chair and read yourself to sleep, several times.

DOMAIN 5:

INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT

> *"Instructor had an excellent knowledge and background in all matters relative to the CISSP, and that knowledge is enhanced by his network skills. It should be noted that I would feel comfortable taking the CISSP today and would likely have studied for another six months if I hadn't taken this course."*
>
> **Dale E. Johnson**

WHAT'S NEW?

ISC^2 published the 3rd edition of their CISSP CBK in late 2012. I ordered my copy in December 2012 and said, "So what's new in Governance and Risk?"

I started going through this domain and only found minor changes.

- The "PUSH" risk assessment methodology has been dropped from the 3rd edition.
- Manage Third-Party Governance is a new section and addresses the areas of:
    - Infrastructure as a service (IaaS)
    - Platform as a service (PaaS)
    - Software as a service (SaaS)
- A section on Tangible and Intangible Asset Valuation has been added:
    - Tangible Asset Valuation
        - Original cost minus depreciation
        - Actual market value through market research
        - Cost of switching to a competing asset or capability
    - Intangible Asset Valuation
        - What is a definite intangible asset?
        - What is an indefinite intangible asset?
        - Cost approximation methods for intangible assets

    - Cost
    - Capitalization of historic profits
    - Cost avoidance or savings
- A section on Vendor, Consultant and Contractor Controls has been added
    - If the third-party is infrequently on site considerations
    - If the third-party is on site for a more permanent basis considerations
    - Regardless of duration, if the third-party has limited access to sensitive information considerations

Also of note, was that the entire section on Ethics has been moved to the Legal domain. But we knew that from having read the new candidate information bulletin for the CISSP.

Along with the usual re-sequencing, these were the areas that received the most work.

An Overview

Now let's take a look at the CISSP Domain that deals with Information Security Governance and Risk Management. When we speak about IS Governance we're talking about how management views security, how the security organization is structured, who the Information Security Officer (ISO) reports to and some basic guiding principles for security. First and foremost, information security is not just about IT. The fundamental principles of security revolve around the CIA triad. No, that's not the Central Intelligence Agency. But rather confidentiality, integrity, and availability. Availability in the sense that the data is available when needed (think about a Denial of Service attack that stops access to your data); Integrity in the sense that the data is accurate and has not been modified (think about your checking account balance, you wouldn't want someone changing that); and finally, Confidentiality (think PII or personal identifying information) your data is confidential, only the people who should know or have access to your private information know and have access.

There has been a lot of talk lately about DAD (Disclosure-Alteration-Destruction) vs. CIA (Confidentiality-Integrity-Availability) so for your information.

When we talk about Confidentiality, we mean the data hasn't been Disclosed.

When we talk about Integrity, we mean the data hasn't been Altered

And when we talk about Availability, we mean the data is there and hasn't been Destroyed

In information risk management there are several concepts that you need to review and understand. First let's look at Q vs. Q or quantitative vs. qualitative risk assessment. If you can determine a specific amount or quantity then it is a quantitative analysis, e.g. the system will be down for 24 hours. It is an objective risk assessment, whereas on the other hand if you can't quantify the variables and the decisions are subjective then the risk assessment is qualitative. There are a number of risk management frameworks, including

- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)
- Factor Analysis of Information Risk (FAIR)
- National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF)
- Threat Agent Risk Assessment (TARA), a recent creation

And you should follow the links above and become familiar with these.

In risk analysis, there are a number of concepts that you will need to understand. First, what is the value of your information and assets? (Asset Valuation or AV) Second, what are the threats against those assets? Third, what are the vulnerabilities associated with those assets? Finally, what is the impact or probability that the threat/vulnerability will have on the organization?

So now here are some formulas that you need to know:

1. Single Loss Expectancy (SLE) is the cost of a single loss and can be calculated by multiplying Asset Value (AV) by Exposure Facture (EF), which is the impact the loss of this asset will have on the organization. SLE = AV * EF
2. Annual Rate of Occurrence (ARO) is how many times you lost an asset.
3. Annualized Loss Expectancy (ALE) is an expression of your annual anticipated loss due to risk and can be calculated by multiplying SLE by ARO. ALE = SLE * ARO.
4. And finally, Risk = Asset Value * Threat * Vulnerability * Impact

Policies, Standards, Procedures and Guidelines

Policies, standards and procedures are required, i.e. you must do these. Guidelines are suggestions, they are optional.

You should be familiar with the different roles and responsibilities in information security including; System Owner, Data Owner, Data Custodian, Security Administrator and System Administrator.

DOMAIN 6:

LEGAL, REGULATIONS, INVESTIGATIONS, AND COMPLIANCE

> *"Excellent instructor. One of the best I have had in over 27 years in the IT business. Genuinely cared about the students understanding the subject material and their success in passing the exam. She taught how to think and reason to pass the test. That is something not found in any text book."*
>
> **Craig Calder**

WHAT'S NEW?

Here are the things that I found different in Legal, Regulations, Investigations and Compliance.

- Ethics has been move from Information Security Governance and Risk Management domain to this domain.
- A new section has been added on "Ensure security in contractual agreements and procurement processes (e.g. cloud computing, outsourcing, vendor governance)"
- New sections have also been added on "Import/Export" and "Trans-Border Data Flow"
- In the section on "Privacy" there is a bulleted list. The 6th bullet point is actually a new paragraph, but somehow it got a bullet instead. That's the one that starts reading "There should be a general policy…."
- The seven principles from the Europe Directive on Data Protection have new titles and definitions. The text alludes to them being EU specific, however, what I found was that the material listed is actually the "Safe Harbor Privacy Principles" issued by the U.S. Department of Commerce on July 21, 2000 and in which DoC specifically states, "The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They

are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States." (SOURCE: http://export.gov/safeharbor/eu/eg_main_018475.asp)

- A new section entitled "Media Analysis" has been added which talks to the process of obtaining evidence from media.
- Still another new section in evidence entitled "Hardware/Embedded Device Analysis" has been added which talks to the analysis of mobile devices such as smart phones or personal digital assistants (PDAs).
- The final new section entitled "Understand Compliance Requirements and Procedures includes sections on:
    - Regulatory Environment
    - Audits
    - Reporting

As always, InfoSec is updating the courseware to reflect this new material and re-sequencing of the Legal, Regulations, Investigations, and Compliance domain.

Now let's look at investigations. From an investigative perspective, you will need to know what constitutes acceptable evidence, how to maintain a chain of custody for evidence gathered, and you should also understand forensics and the things that could invalidate the evidence in a court of law. Always remember when gathering forensic evidence, the goal is to be able to present acceptable evidence in a court of law. You will not go to court with every piece of evidence that you gather. But you should be prepared for the eventuality.

For an ethical point of view we have the following rules written by the **Computer Ethics Institute**:

- Thou shalt not use a computer to harm other people.
- Thou shalt not interfere with other people's computer work.
- Thou shalt not snoop around in other people's computer files.
- Thou shalt not use a computer to steal.
- Thou shalt not use a computer to bear false witness.
- Thou shalt not copy or use proprietary software for which you have not paid.

- Thou shalt not use other people's computer resources without authorization or proper compensation.
- Thou shalt not appropriate other people's intellectual output.
- Thou shalt think about the social consequences of the program you are writing or the system you are designing.
- Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Most importantly, for this exam, familiarize yourself with ISC^2 © Code of Ethics.

So what else can I say about the Law, other than it is the Law and we must abide by it, or suffer the penalties.

One final parting comment, look up the definitions of and differences between 1) due care, 2) due diligence, 3) due process and 4) due protection.

AN OVERVIEW

There are several topics we need to look at when we discuss the Legal domain of CISSP. First you need some background and a couple of important distinctions:

Civil Law and Common Law — The most significant difference is in civil law judicial precedents and particular case rulings do not have the same weight as they do under common law.

Civil Law and Criminal Law — The significant difference here is in the burden of proof. In criminal law, the standard of proof is "beyond a reasonable doubt." However in civil law all that is needed to prove a case is a preponderance of the evidence to be in your favor.

In which of the aforementioned can a possible punishment be jail time? Only criminal law.

If you see Australia in the test question, look for common law in the answer set since common law is the legal system used in the United States, Canada, the United Kingdom and most former British colonies (that includes Australia).

To satisfy your curiosity, look up criminal law, civil law, and common law and write down the definitions. And while you're there look up statutory, compensatory, and punitive damages. Should you see those terms, you'll be familiar with their definitions.

There are also some definitions with regards to intellectual property law that you will need to know, things like; trademark, copyright, licenses, trade secrets and patents.

The term we come across most often of those is licenses. How many copies of a particular software package are you licensed to use and what are the penalties if you get caught using pirated software? You also need to understand import/export restrictions especially as they apply to crypto systems and hardware.

Some of the other topics under this domain include specific laws, investigations and ethics.

First, let's look at specific laws. You should have an understanding of the general requirements of these laws and where they might be applicable:

- HIPAA – Health Insurance Portability and Accountability Act
- Computer Fraud and Abuse Act – Title 18 Section 1030
- Electronic Communications Privacy Act
- Patriot Act of 2001
- Gramm-Leach-Biley Act (GLBA)
- Sarbanes-Oxley Act of 2002
- Payment Card Industry Data Security Standards version 2.0
- Family Educational Rights and Privacy Act of 1974 (FERPA aka. The Buckley Amendment)

There are also a number of different Breach Laws which, at present, are only at the state level.

DOMAIN 7:

SECURITY OPERATIONS

"OMG!! My instructor is can dance circles around Shon Harris. Nothing against Shon but my instructor was excellent. She explained the most important and hard to understand topics which even today I can still remember and makes good since. I am able to apply what I learned into the real world."

Mark Whiting
US Mint

WHAT'S NEW?

As I said, you can take that for what it is worth; the information remains the same.

Big change, this domain has been renamed. It was changed from **Operations Security** to **Security Operations**.

Here are the things that I found different (new and added).

- A full page was added which explains "**Need to-Know/Least Privilege**."
- Under privileged accounts, "Root or built-in administrator accounts", "Power Users" and "Administrator accounts" have the following additional sentence at the end of the description. *"These accounts should always be considered for multi-factor authentication methods such as one-time pads."*
- Power Users also has several additional lines dealing with the management of power user accounts.
- A half-page was added to the end of System Administrators and Operators outlining:
    - Least Privilege
    - Monitoring

  - Separation of Duties
  - Background Investigation
  - Job Rotation
  - In the section on Monitor Special Privileges, the concept of "whole person" was added while talking about background checks as well as a couple of extra bullet points on repeated patterns of high-risk behavior and illegal activity
- A half-page was added to explain **"Job Rotation"**
- The Marking paragraph got some extra language on how labels should be written.
- A full page was added to explain **"Record Retention"**
- In the Media Management section a full page was added for **"Removable Media"** and two pages on **"Disposal/Reuse."**
- **"Asset Management"** got its own section and two pages of information.
- Response, Reporting, Recovery, Remediation and Review, including Root Cause Analysis got their own 4-page section
- **Configuration Management** was updated to include software and software inventory concerns
- In the section on Drives and Data Storage, **SAN and NAS** got an additional 10-lines of info.
- As always, InfoSec is updating the courseware to reflect this new material and the re-sequencing of the Security Operations domain.

An Overview

Operations Security (OpSec) is concerned with the same basic elements as all the other CISSP domains and those are confidentiality, integrity and availability.

So let's approach OpSec from that CIA perspective: How do we keep the data and systems confidential, maintain integrity and ensure they are available? There needs to be controls for both the data and the people who have access to the data. And, those controls need to be monitored for effectiveness as well as to determine if any incidents have occurred.

When looking at staff, we need to ensure that background investigations are being performed for anyone with access to sensitive data, we need to enforce the taking of vacations; we need to plan for and execute job rotation; and we need to remember to grant access based on the principle of least privilege. Only give the person access to the data they need to do their job and do it using RBAC (role based access control). RBAC makes it a lot easier to add and/or remove access since you only have to remove the rule to effect the change. Job rotation and enforced vacation taking are both controls used to prevent/deter fraud. Ensuring that each person also has a separate sign-on helps to enforce accountability. And while we're monitoring the people and their access, you need to know the definition for "CLIPPING LEVELS" and how it might be used. For example, we might set the audit software to only report failed login attempts if there have been more than five for a single user within a one hour time period. Which, by the way, could be an indication that a password attack was underway.

Before we talk about the data, let's look at the hardware/software side of OpSec briefly. There needs to be system controls in place to help the operations staff when it is time to reboot, patch, upgrade, run backups or run daily jobs. There needs to be controls… No, make that CHANGE CONTROLS in place regarding hardware maintenance, even down to the point of reconfiguring the hardening of a particular server. Nothing, and I repeat nothing, should be done to a piece of hardware without an approved change control, signed by the appropriate management representative. And, the change should be vetted in a test environment and NEVER directly into production.

Two other rules for hardware:

- Vendors should be required to come on site to make changes or upgrades and only if they have an approved change request, notice I stated they should come on site — that eliminates all the remote access issues for vendor maintenance.
- Those vendors should be escorted by someone in OpSec, familiar with what's being done. We don't want the vendors making random hardware re-configurations just because they happened to be on site.

Another key concept here is that the escort should be knowledgeable, otherwise the vendor can feed them a line of meaningless chatter and proceed to change whatever they want. Here's a good scenario question for you. The vendor comes on site and says, "You have a bad drive in your RAID array. I've replaced it with a brand new one and all the data has been restored. I'll take the old one back with me so that you don't get charged the shipping fee." Should you allow this? The answer should be NO. To protect the confidentiality of data which may or may not be stored on that drive, you need to put it through your own sanitization procedures and not rely on the vendor. I realize it's a stretch, but that is a good example of Data Leakage.

And speaking of maintenance in OpSec, you'll need to understand Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) as part of the disaster recovery process for OpSec.

Data — like people — also need the principle of least privilege, in that only people who need to see it should be allowed. It needs to be backed up and stored offsite to help OpSec achieve the RTOs and RPOs defined by the user in their Business Impact Analysis. Just as an aside, what is a "safe distance" when it comes to defining where data will be stored offsite? My definition is that the event which caused the disaster will not affect the offsite storage location, if it does then it's too close.

Like most other areas, OpSec also needs to have its own continuity of operations plan. How will they continue to do business if the IT infrastructure is inoperable? Let's say just one array of disk drives are down and the vendor has a four-hour response window, the question is, what do you do during those four hours while you're waiting for the vendor to fix the hard drive? What is your incident response plan? Speaking of which, and as the last item, every OpSec group needs to have a very thorough incident response plan. Who do you contact if there is an incident? What if it's 3:00AM on a holiday morning? What if it's on the late night shift and the other operator has gone to dinner and you're the only one in the computer room? All of these need to be spelled out in an incident response plan.

And… that IR plan along with the COOP and DRP need to be tested — frequently.

Domain 8:

Physical & Environmental Security

> *"Without a doubt one of the best instructors I have had the privilege of to attend a course of instruction with. He is both methodical, relevant, and has a repository of core knowledge and background that made the material simple(r) to digest and use in a testing environment as well as applying those principles in my day to day routine. Great class, great instructor."*
>
> **Adrian Young**
> **USCG**

What's New?

Here are the things that I found different in Physical (Environmental) Security.

- New Pictures (almost all have been updated).
- The American Institute of Architects list of key security concerns has been expanded from 9 to 19, and now includes:
    - Facility security control during and after hours of operation
    - Personnel and contract security policies and procedures
    - Personnel screening
    - Site and building access control
    - Video surveillance, assessment, and archiving
    - Natural surveillance opportunities
    - Protocols for responding to internal and external security incidents
    - Degree of integration of security and other building systems
    - Shipping and receiving security
    - Property identification and tracking
    - Proprietary information security
    - Computer network security

    - Workplace violence prevention
    - Mail screening operations, procedures, and recommendations
    - Parking lot and site security
    - Data center security
    - Communications security
    - Executive protection
    - Business continuity planning and evacuation procedures
- A new section on "Personnel Privacy and Safety" has been added and includes subsections on:
    - Privacy
    - Travel
        - You Should Know
        - Before You Travel
        - Prepare Your Device
        - While You're Away
        - When You Return
    - Duress

As always, InfoSec is updating the courseware to reflect this new material and re-sequencing of the Physical (Environmental) Security domain.

AN OVERVIEW

This week's article looks at the Physical and Environmental Security domain of CISSP. First and foremost, (ISC)^2 and the CISSP exam consider human safety paramount. If you have a test question and one of the answers is human safety, that is the right answer, it is always MOST important.

Let's talk about the physical. Physical Security means just what it says, securing the physical perimeter. Define who has access to the physical site, whether it is the entire building housing your data center or simply a self-contained room which contains your servers. Remember and follow the simple rule we defined for firewalls, deny all. No one gets access to the server room, and then only permit the people in who have a need to be there. And that doesn't include someone who's using the server room as storage for paper files. But that's an environmental issue and we aren't there yet.

The other thing to remember about physical access is that there will be times when vendors need to be physically present to perform maintenance or diagnostics. Those vendors should always be escorted by someone who is on the approved access list. You'll need to maintain a log of who entered at what time, and when they left. Speaking of the approved access list, like other access lists you need to have a review process in place, which periodically looks at who is on the approved list and whether they should continue to have access.

Depending upon your level of security, the physical design could include things like external boundary protection. Bollards preventing someone from driving their car through the front door, fencing, guard dogs, and perhaps armed guards — now this is really paranoia at its best. But seriously, at Federal Courthouses, I've seen bollards in the middle of the driveway to enter the building. By the way, you already know what a bollard is, though you may not know its name. Google it if you don't know what a bollard is.

Your security awareness training plays into successful physical security access as much as it does anywhere else. For example, say it's raining and you're walking towards the passcard protected door to go into the data center and there's a person walking alongside you — who you don't know. Their hands are full with an umbrella, a lunch bag, a gym bag, a computer bag, some books and maybe even a box of Krispy Kremes. Being polite, what do you do? You hold the door open for them, of course. Wrong. That's piggybacking in its simplest form.

Now when we talk about Environmental security, we're talking about the basics: electricity, water, fire, natural phenomena, and even unnatural phenomena.

Electricity basics to be aware of: no single point of failure; two feeds from different power sub-stations; UPSs; generators; and, of course, batteries. You should know the difference between voltage regulators and surge protectors; the difference between voltage spikes, sags, faults, and brownouts; the role UPSs play in the electrical scheme of things; how long it takes for your generators to come online and how long your batteries should last.

Water basics: If it's brown don't drink it. Just kidding. But you should be aware of moisture detection and prevention as well as acceptable humidity ranges. You should also know the difference between wet pipe and dry pipe fire extinguisher systems. You should also be familiar with the newer WADSC — that's short for Water Alert Detection Sensor Cable.

Fire basics: Halon is no longer in vogue. In fact, it is against the law to use. Hand-held fire extinguishers should be visible, inspected, of the appropriate type, and the people who have access to the data center should be trained to use them. Know the classes of fire extinguishers and fires: A, B, C. The computer room is NOT a storage room for paper files, that's adding fuel to your potential fire. Besides everyone will then be wanting to get in the computer room to get a file out of a box. Do you really want to go digging through boxes looking for files when you could be testing your NIDS? Of course not.

Natural phenomena: Hurricanes, tornadoes, earthquakes, and other sorts of dangerous weather present different damage risks. Remember YOU might not suffer any actual damage, but the supporting environment (power lines, phone and data lines, or even roads) may not be working for awhile. This basically means you should have a proactive incident response plan. If a tornado alert is issued, what do you do?

Non-natural phenomena: Civil disturbance, disgruntled employee/contractor/customer, terrorist attack, biological attack, airborne agents or something as simple as the flu can negatively affect physical security. What's your backup plan if a vendor needs to get into the computer room and everyone who is authorized to access the server room is out, either sick or on vacation? How do you handle airborne agents – let them dissipate.

And as a final note, using your facility as a training facility for the volunteer firefighters and/or volunteer ambulance group can work wonders for establishing a rapport with the local community. Just remember, only those that have a need to know should be allowed into the most secure areas.

And as is always the case, test your disaster recovery plans, contingency plans, and incident response plans. Then critique them after the test and update them as necessary.

DOMAIN 9:

SECURITY ARCHITECTURE & DESIGN

> *"I was amazed at the instructor's knowledge of the material as well as his ability to teach the material. I would give every aspect of the course a 10. Great Class!!"*
>
> **Larry Thompson Jr.**
> **The Pentagon**

WHAT'S NEW?

One thing I noticed different about this domain is that instead of "Section Summaries", that information has been moved to the beginning of the section and has various titles, all of which mean "Section Introduction." The information is relatively the same.

Here are the things that I found different in Security Architecture & Design.

- The section on "Security Zones of Control" now has diagram (Figure 6.2) from NIST which illustrates the concept of using a subsystem guard. Part of the work of the (Joint Task Force Transformation Initiative Feb, 2010)
- In the 2nd Edition, where they were talking about "Multilevel Lattice Models" there was a second paragraph which explained how noninterference models could be considered a type of multilevel model. For some reason, in the 3rd Edition, rather that include that as a second paragraph, it got its own bullet-point, but it isn't bolded, because the very next bullet-point is bolded and it is Noninterference Model. I think someone just did an "oops" on this.
- Finally, something we can say is "NEW." They added a couple of pages on the Payment Card Industry Data Security Standard in the section on "Industry and International Security Implementation Guidelines."
- Other new material which has been added, includes a section on "Virtualization"; and four pages on "Vulnerabilities of Security Architecture" which includes:

  - System design
  - Emanations
  - State Attacks
  - Covert Channels
- Also included is a complete section on Software and System Vulnerabilities and Threats, which includes:
- Web-based
  - XML
  - SAML
  - OWASP
- Client-Based Vulnerabilities
  - Desktops, Laptops and Thin clients
  - Mobile Devices
- Server-Based Vulnerabilities
- Data Flow Control
- Database Security
  - Warehousing
  - Inference
  - Aggregation
  - Data Mining
- In the section on Distributed Systems, a lot of good information has been added, including sections on:
  - Grid Computing
  - Cloud Computing
    - On-demand Self-Services
    - Broad Network Access
    - Resource Pooling
    - Rapid Elasticity
    - Measured Service
- Service Models
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- Deployment models
  - Private Cloud

- Community Cloud
- Public Cloud

As always, InfoSec is updating the courseware to reflect this new material and re-sequencing of the Security Architecture & Design domain.

AN OVERVIEW

This article will cover some of the major areas within Security Architecture and Design by looking at: design concepts, hardware architecture, OS and software architecture, security models, modes of operations, and some system evaluation methods, specifically CAP.

First, design concepts. You need to remember "LAST." That is L=Layering, A=Abstraction, S=Security Domains and T=The Ring. Actually is should have been LASR but who could remember that and besides if you vocalize THE RING it sticks with you. OK, so layering or separating the design into distinct parts like hardware, hardware drivers, operating system and application. Abstract, like in abstract painting, you never really know what the artist was thinking because all of that is hidden from you the viewer/user. As an example, if you click on a URL in your browser, say for infosecinstitute.com, you as the user see the web page painted on your screen, you don't see all of the electronic work going on in the background to handle communications like file lookup, screen painting, etc. You just see the screen. In Security Domains, think two things, user mode and supervisor mode. Users can only do what they have been allowed to do and supervisor mode can do anything. And finally, THE RING. No not the one you give to a very close acquaintance. But rather how security is designed, the closer to the center of the ring the more restrictive the security.

Next, hardware architecture. Now, we already know the basics about input devices, CPUs, output devices, memory, hard disks, etc. So I won't bore you with that minutia. But you should Google the following subjects: pipelining, interrupt, processes, threads, multitasking, multiprocessing, SRAM, DRAM, virtual memory and WORM — not the virus, but write-once, read-many. Once you've Googled those, cut and paste the definitions you find somewhere and keep them handy.

Then, OS and software architecture. You need to understand the "reference monitor" and the role it plays in mediating access. You should be able to look at UNIX/Linux permissions and know the difference between Owner/Group/World and who has what. Also, look at NTFS permissions in Windows and get a good grasp of the differences between the five different levels of permissions. Some key words to research and remember in this section are: TOCTOU, backdoor vs. maintenance hook, and don't forget polyinstantiation.

For security models, you can read through the different models, but pay particular attention to the Biba model and the Bell-LaPadula model and how they work with the principle of least privilege.

There are four different modes of operation; multilevel, compartmental, system-high and dedicated. Understand the role of the reference monitor in the multilevel mode.

And finally system evaluation methods or as we like to call it Certification Accreditation Program (CAP). (ISC)^2 is getting away from asking questions which ask you to classify levels by ITSEC but it wouldn't hurt to familiarize yourself with the Common Criteria and the EAL levels, especially the difference between EAL3 and EAL4 and the difference between EAL5 and EAL6 (remember verify, verify, verify). And remember it all started with the Orange book (no network) and then went to the Red book (included network).

DOMAIN 10:

TELECOMMUNICATIONS & NETWORK SECURITY

> *"I thoroughly enjoyed the class. The instructor teaching skills added immensely to the course material to ensure her students were grasping the material. I would absolutely recommend."*
>
> **David Mart**

WHAT'S NEW?

I started going through the Telecommunications and Network Security domain and "WOW!!!" My hat's off to the people who put this domain together.

In the 3rd edition, there are four main sections:

- Secure Network Architecture and Design
- Securing Network Components
- Secure Communication Channels
- Network Attacks

Compare this to the 2nd edition, which had eight sections:

- Introduction
- Layer 1: Physical Layer
- Layer 2: Data-link Layer
- Layer 3: Network Layer
- Layer 4: Transport Layer
- Layer 5: Session Layer
- Layer 6: Presentation Layer
- Layer 7: Application Layer

You can tell just by looking at the index that the emphasis has changed from the old OSI model to a "new way of thinking" about network security. When I was looking at the Network Layer and found that 3rd edition went into detail regarding RIPv1 and RIPv2, as well as OSPFv1 and OSPFv2 I was OK with the level of detail, what I found impressing was how "easy" it was to read and understand. Even when it went into all the protocols associated with the Network Layer, I found it "easy" to read. But on to some good stuff; check out SASE and CASE in the Presentation Layer.

I noticed that this new edition also contained SCADA, which I found to be quite factual and straightforward. It is of interest to note the vulnerabilities in the reference table on page 312.

Multimedia collaboration and spimming, I think I need a new dictionary. Even SEM and SEIM, no wait a minute that should be SIEM. That is of course, unless they are coining a new phrase. I'm going to stick with SIEM, Security Information and Event Management. In any event, in the Telecommunications domain they refer to Security Event and Incident Management but talk about SIEM devices. Maybe it's just a typo, you know how those things happen.

I like how the "Attack" section was organized. It clarified some things for me.

For me this domain is well organized, well highlighted, and as I said before, an "easy" read. There is however, way too much information in this domain to include it here, you'll simply have to get the new CISSP CBK and read this domain.

AN OVERVIEW

Telecommunications and Network Security is this week's CISSP domain posting.

The dreaded OSI model, there's no way around it, PDNTSPA or Please Do Not Throw Sausage Pizza Away, or **P**hysical, **D**ata Link, **N**etwork, **T**ransport, **S**ession, **P**resentation, and **A**pplication. This one you've just got to memorize and know what happens at each layer, and then once you get that down and you know which networking devices operate at which level, you can switch gears and go to the TCP/IP model. The TCP/IP model is NITA (Now It's Totally Awesome). No that's not "need a" (as in a drink) it's NITA or Network, Internet, Transport and Application. So here's the comparison:

	OSI MODEL	TCP/IP Model
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Transport
3	Network	Internet
2	Data Link	NetworkAccess
1	Physical	

And remember, you need to know which networking devices operate at which layer. For example, which layer do routers work at???? Hint (3)

For TCP/IP you need to understand IPv4. Know the Private Addresses, there're three of them. And you'll need to know the advantages of IPv6. So the trick question is, since the address range of an octet within the IPv4 addressing scheme is 0-254; is 10.10.10.255 a valid IP address and if you say yes, then what is it used for? In IPv6 what does "::" represent. The answer=nothing. Actually it's zeroes. But same difference.

You should understand the differences between Analog and Digital communications; between Asynchronous and Synchronous; and between broadband and baseband. Speaking of analog communications, what is the major disadvantage of using modems? Answer: They can be used to circumvent your firewall and IDS/IPS devices.

For the area networking conversation, you need to know the traditional terms LAN, WAN, MAN, PAN, WLAN, PWLAN, etc. You'll also need to know the configurations of BUS, STAR, RING, and MESH. A good question is in which configuration would you most likely find a Hub.

And speaking of hubs, let's talk a little about the different devices you should be on speaking terms with. Namely they are hubs, switches, repeaters, bridges, gateways, PBXs, firewalls and honeypots just to name a few. You'll need to figure out which ones simply forward all traffic; which ones filter traffic based on MAC address and which ones are easiest to hack.

In some of the services and protocols, check out DNS, particularly read the details behind zone transfers and how they work. Then look at DHCP, Active Directory services, LDAP and Kerberos. Pay particular attention to which ports Kerberos uses and which protocol is used for communicating between the client and Kerberos.

Remote access is getting a lot of attention from (ISC)2, so pay particular attention to how RADIUS authenticates, why ISDN (It still does nothing) isn't a good choice, why VPN is rapidly becoming the de facto standard for secure remote communication and why modems should NEVER be allowed in your network.

Wireless, ah wireless. It's everywhere. Most establishments advertise "FREE WIFI" And each time a security professional sees that they cringe, it's like hanging a sign around your neck saying here are my userid and password credentials. But seriously, let's take a look at some of the topics you'll need to become familiar with for the exam. So for a laundry list of acronyms, WEP, WPA, WPA2, 801.x (and all forms of 801 – 802.11 including A,B,G,N,I) and let's not forget SSID. Don't broadcast the SSID. That's the answer, you just have to remember it when you get to the question on the exam. You'll also need to understand WARDRIVING and WARDIALING and air sniffing. Oh, and before I forget, let me answer by Blackberry with my remote earphone using Bluetooth. Several questions are showing up on Bluetooth including bluescanner and bluesniffer. I've even seen some questions on a more recent version which deal with Apple's wireless communication for iPads.

As a final note, instant messaging (IM) falls under the realm of network security and you will need to understand the implications of sending sensitive data via IM. In a word, DON'T!!!!

Infosec Institute's Cissp Boot Camp

Course Overview

Our Course Page: http://www.infosecinstitute.com/courses/cissp_bootcamp_training.html

Our CISSP course is always updated to comply with the most current (ISC)² CISSP exam. If you are prepping for the exam, rest assured that you will have the best and latest materials and exam preparation in the industry.

InfoSec Institute provides this highly-rated 7 Day CISSP Boot Camp to the Information Security community. The CISSP Boot Camp trains and prepares you to pass the premier security certification, the Certified Information Systems Security Professional (CISSP®). Professionals that hold the CISSP have demonstrated that they have deep knowledge of all 10 Common Body of Knowledge Domains, and have the necessary skills to provide leadership in the creation and operational duties of enterprise wide information security programs.

InfoSec Institute's proprietary CISSP certification courseware materials are always up to date and synchronized with the latest (ISC)² exam objectives. Our industry leading course curriculum combined with our award-winning CISSP training provided by expert instructors delivers the platform you need in order to pass the CISSP exam with flying colors. You will leave the InfoSec Institute CISSP Boot Camp with the knowledge and domain expertise to successfully pass the CISSP exam the first time you take it.

When you enroll in an InfoSec Institute CISSP Boot Camp in either our classroom-based or live online boot camp, you are eligible for our CISSP Dual Certification program at no extra cost. You have your choice of focusing on management with the ISSMP, a focus on security engineering with ISSEP or a focus on security architecture with ISSAP. Demonstrating additional proficiency in one of these areas is a way for you to quantify your security experience in the form of a highly regarded ISC2 certification, as well distinguish yourself from the other 83,000 CISSP certification holders.

Course Schedule

View the CISSP schedule here or see our full course schedule.