Risk Management Approach to Security Authorization

Table of Contents

Objectives ........................................................................................................................................ 3
Definitions -1 ................................................................................................................................... 5
Definitions -3 ................................................................................................................................... 6
Definitions -4 ................................................................................................................................... 7
Definitions -5 ................................................................................................................................... 8
Definitions -6 ................................................................................................................................... 9
Definitions -7 ................................................................................................................................... 10
Definitions -8 ................................................................................................................................... 11
Definitions -9 ................................................................................................................................... 12
Definitions -10 ................................................................................................................................. 13
Definitions -11 ................................................................................................................................. 14
Definitions -12 ................................................................................................................................. 15
Definitions -13 ................................................................................................................................. 16
Definitions -14 ................................................................................................................................. 17
Definitions -15 ................................................................................................................................. 18
Definitions -16 ................................................................................................................................. 19
Definitions -17 ................................................................................................................................. 20
Definitions -18 ................................................................................................................................. 21
Definitions -19 ................................................................................................................................. 22
Definitions -20 ................................................................................................................................. 23
Definitions -21 ................................................................................................................................. 24
Objectives

Understand the difference between applying risk management principles and satisfying compliance requirements

Be able to identify and maintain information systems inventory

Understand the criticality of securing information

Understand organizational operations

**012 What is the difference between looking at things from risk management and security compliance? Anybody tell me? Risk management versus security compliance.

Student: I'll take a stab and this will probably be lay terms but my view is that risk management is looking at what are the security concerns that you have and saying which ones do I care the most about. Which ones are going to affect my business? Which ones are going to affect the bottom line? Whereas security management might be just oh, I patched this system. I’ve patched all these systems. I’ve patched some percentage of my systems, but that doesn’t mean that
that aligns necessarily with what the risks are to the overall mission.

Ben Malisow: Yeah, yeah. Basically risk management is looking at it from a holistic view of what is the real threat? What is the real risk? What is it that we have to look at? Security compliance is usually here’s a set standard that you have to live to. This standard was created by an external entity that is not familiar with your operations or your business or your goals. You have to live by this whether or not it’s applicable to you.

There are good and bad things about both. Okay, there’s no one real answer, but obviously (ISC)2 likes CAP. They like the RMF, they like the risk-based assessments. Make sense?

These are the objectives that we'll look at in this module. You'll be able to identify and understand the information systems inventory as if you don't know that already you should. Criticality of securing information, and understanding your organizational operations which is very important in terms of the risk management structure.
**013 What is information security? What is it? And yes, lay terms are fine by the way. I haven't been spouting a lot of technical babble yet, have I? Okay good. What is information security? What is it? It's not a trick question, Bob?

Student: Keeping your information secure.

It's protecting your information from unauthorized access, disclosure. It's your CIA triad, all the CISSPs know that, right? Let's break that one down: confidentiality, integrity and availability.
**015 Availability is what? What are you trying to do when you make sure that your information is available?

Student: Accessible.

Ben Malisow: Yeah, yeah. Is that you can get to it when you need it, right? Yeah.
Definitions -4

Availability – The ability to use the information or resource when it is needed

Integrity –

Confidentiality –

Ref: NIST SP 800-37 Rev-1, Appendix B

**016 If you can't, if you have unauthorized down time or unscheduled down time that's going to impact your operations.

What's integrity?

Student: It hasn't been modified or tampered with.
**Definitions -5**

**Availability** – The ability to use the information or resource when it is needed

**Integrity** – Describes the wholeness and completeness of the information without any alteration except by authorized sources

**Confidentiality** –

*Ref: NIST SP 800-37 Rev-1, Appendix B*

**017 Ben Malisow: That's like a textbook answer right there. Good. See what happens when he doesn't just restate the answer?**

Okay confidentiality. What's confidentiality?

Student:
Ben Malisow: Only authorized people have seen it. It's as secret as you need it to be.
**Availability** – The ability to use the information or resource when it is needed

**Integrity** – Describes the wholeness and completeness of the information without any alteration except by authorized sources

**Confidentiality** – Ensuring information is only available to those authorized to have access to the information

*Ref: NIST SP 800-37 Rev-1, Appendix B*

**018 Good, good. And that’s our CIA triad or in this case, AIC, flip it around a little bit. Any test you take, I don’t care if it’s (ISC)2, I don’t care if it’s ISACA. I don’t care if it’s Security Plus, these three things, this triad right here are a good 40 percent of the answers. I’m not going to teach the test but that’s in fact the case.*
**019 Security Controls Assessment.
Anybody tell me what that is just by what those three words mean?

Student: You don't have to throw candy at me. But again, assessment is some way of looking at evaluating what you've got, so if you take Katie's approach and look at that backing out of it then what you're doing is here's a system for this system. These are the sets of controls that I need to have that are related to security so how well do I stand up against them?

Ben Malisow: She did pretty good, didn't she. You sure you don’t want a candy?

Student: Yeah I'm sure.
Definitions -8

**Security Controls Assessment** – The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.  

*Ref: NIST SP 800-53A Rev-1, Appendix B*

Authorization –

**020 Ben Malisow: Alright, that's exactly it. That's exactly it. You're testing those controls. You're making sure they're doing what you want them to do inside your system, right? And we're going to talk about the different kinds of controls and how they're implemented a little bit later.

Authorization. What's authorization?

Student: Being granted permission to access?

Ben Malisow: Yes, yeah.

Student: Based on somebody who's got the authority to give it.
Ben Malisow: Yes and from a user perspective that's how we do system access in our grand RMF scale, in our CAP concept, authorization will be the authorization to run the system, to actually operate it. And we’ll get deep into that in a little while too.

**021 And on all these slides we tried to go to refer to the source material where these actual definitions came from in case you're interested and want to do some more examination of that and they should all match up to the slides that you have.

**Definitions -9**

**Security Controls Assessment** – The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.  
*Ref: NIST SP 800-53A Rev-1, Appendix B*

**Authorization** – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.  
*Ref: NIST SP 800-37 Rev-1, Appendix B*
**022 Alright, reciprocity. A nice 25-cent word. Whoo-hoo. Anyone know what the word means in general, not even in terms of IT systems. Yeah?

Student: I'll give to you what you give to me.

Ben Malisow: Exactly, that's exactly it. Same-same, right? Same-same, sharing. In terms of our systems reciprocity means I'm going to trust your system as much as you trust my system. And if we have this shared amount of trust built in then we can exchange information at the same level with the same confidence. Does that make sense? You don't want- because if you pass your information to somebody
else who is less secure, you’re just basically giving it away, aren’t you?

Student: Bank-to-bank transactions.

**Definitions -11**

Reciprocity – Mutual agreement among participating organizations to accept each other’s security assessments in order to reuse information system resources, and/or to accept each other’s assessed security posture in order to share information.

*Ref: NIST SP 800-37 Rev-1, Appendix B*

**023 Ben Malisow: Oh bank-to-bank is huge.
All they have to lose is money though.**
**024 What is an Information System? Low hanging fruit. Come on Katie. Come on now. Is it a system for containing information? Don't do it! Don't you dare.

Student: It's where you store-

Ben Malisow: Yeah.

Student: Your company framework information.

Ben Malisow: Data, sure, sure.

Student: Data.
Definitions -13

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Ref: NIST SP 800-37 Rev-1, Appendix B

General Support System (GSS) –

**025 Ben Malisow: Processing, maintaining, storing, all that stuff. It is if you look at it in the bit picture, it’s not just the bits and the bytes, it’s not just the hardware and the software. It’s the people and the processes too. They’re all part of the system.

GSS, General Support System is a little bit more arcane in terms if the definition.
**Information System** – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

*Ref: NIST SP 800-37 Rev-1, Appendix B*

**General Support System (GSS)** – An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

*Ref: OMB Circular A-130, Appendix III*

**026 It comes out of OMB Circular A-130 where it’s very much similar to an information system. But it’s more about the bits and the bytes. It’s more about the hardware and the software.**
**027 Major Application. These are kind of these are not intuitive either and they’re not often obvious industry terms. Anybody know what they’re going for when they say ”Major App”? Anyone want to take a guess at it? Georgia? Oh you’re going to defer to Michael, okay.

Student: Application go down would wind up causing harm to the.

Student: Sounds like Snicker time.

Ben Malisow: Snicker boy, welcome to the team. Okay yes, yes. Not just cause harm to the organization but cause serious or grievous harm to the organization.
Definitions - 16

**Major Application** – An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

**Minor Application** –

**028 Something that is critical. And not necessarily in the medical term of critical where somebody might die but that could be considered a major application. Minor Application of course is the opposite. Those are your admin systems, your support systems.**
Definitions -17

**Major Application** – An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

**Minor Application** – An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

*Ref: NIST SP 800-37 Rev-1, Appendix B*

**029 Things that if they went down it would be annoying but not necessarily devastating. Are these things the same for every organization? Why not? Why not? Who really cares about the phone bank? Isn't the phone bank always just a minor app?**

Student: Not if you're 9-1-1.

Ben Malisow: Not if you're-- you don't want another candy, do you? Okay yeah! Not if you're Fed Ex right? Those are your major apps depending on what your organization does and that's how you to have to define what you're going to secure, right? Good answer.
**030 Threat, what's a threat?**

Student: Something that can act negatively against anything else.

Ben Malisow: That's it. Something that could hurt you. Something that could hurt you. That's all a threat is, right? Something that might hurt you. Good.
**Definitions -19**

**Threat** – Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

*Ref: NIST SP 800-53, Appendix B*

**Vulnerability** –

**031 Vulnerability?**

Student: Weakness.

Ben Malisow: Weakness. The way the threat is going to hurt you. They way they're going to get in right? Good. Good, excellent.
Definitions

**Definitions**

**Threat** – Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

*Ref: NIST SP 800-53, Appendix B*

**Vulnerability** – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

*Ref: NIST SP 800-37 Rev-1, Appendix B*

**032 First word in that definition.**

Good job.
Risk –

Risk Assessment –

**033 Risk. Risk. The likelihood that the threat is going to exploit the vulnerability. Right?
Risk – The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment –

**034 Good, and a risk assessment?**

Student: Measurement of that.

Ben Malisow: Good, yeah.
**Definitions**

**Risk** – The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

**Risk Assessment** – The process of identifying risks to agency operations, agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

*Ref: NIST SP 800-30, Appendix E*

---

**035** It's a way to try to accurately gauge whether or not a particular risk is going to bear fruit, right? Good, good.

Student: That's my car.
**036 Ben Malisow: Isn’t that great? Do you have one of those?

Student: I do.

Ben Malisow: Do you have the lock?

Student: No.

Ben Malisow: I was going to say that’s pretty cool. I want to come out to the parking lot and see that. Why does that piece of clip art go so well with the slide for adequate security? What’s adequate security?

Student: Well adequate is something that will deter the walk-by, drive-by attacker.
So it’s secured but it’s not totally secured. Like that bracket will stop the casual criminal but you could come by with a lift and lift it right out.

Ben Malisow: Okay all right. Adequate has to be significant enough to protect you. Is there a flip side to adequate? Is there an opposite to that?

Student: Basically if that picture instead of having it going over a tree it was over like a fire hydrant.

Ben Malisow: Okay but I think that's still the same-- that’s hitting your minimum floor of security.

Student: Well but I think what he's saying is that if it’s a fire hydrant all you have to do is lift-

Ben Malisow: Lift the thing up. It would be inadequate. Right, right. That would be inadequate because it's not hitting that minimum level.

Student: Right.

Ben Malisow: Is there an opposite way of looking at adequate security? Let me put this out there. How many of you have a meteor shield on top of your building?

Student: Not me.

Ben Malisow: Why not? Aren't you afraid of meteors, right? Is there a risk that a meteor could strike your building?

Student: Absolutely.

Student: Yes.
Ben Malisow: Yes. Is it significant?

Student: Catastrophic.

Student: Yeah.

Ben Malisow: That would be a pretty bad threat wouldn’t it? What’s the likelihood?

Student: Very little.

Ben Malisow: Yeah. Would putting a meteor shield on your roof be adequate security? No, no, because you’re over arching. Now you’re hitting a ceiling. Somewhere in between that floor and that ceiling is your adequate security because otherwise you’re overspending and it’s disproportionate, right? I mean right there, does that lock look more expensive than that car? No offense to your vehicle.
**Adequate Security** – Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

*Ref: OMB Circular A-130, Appendix III*

**037 But yeah, plus, where do you put the thing? I mean does it go in the trunk? What do you do with that? Just the key would be a pain in the neck right?**
Risk Management vs. Compliance

**Risk Management** – The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system, and includes:

- The conduct of a **risk assessment**;
- The implementation of a **risk mitigation strategy**; and
- Employment of **techniques** and **procedures** for the continuous monitoring of the security state of the information system.

**Compliance** is essential to **ensure** that those **techniques** and **procedures** are being **followed** in the manner intended.

**038 So risk management. It’s the process that we use to try to determine what that risk is to our operation. We use this three way phase of doing that. Conduct the risk assessment. Find out what the risks are, what the likelihood is that those threats are going to exploit those vulnerabilities. We come up with our risk mitigation strategy. Why not "Risk Elimination"? Why "Risk Mitigation"?

Student: Because some you can’t eliminate.

Ben Malisow: There’s no such thing as zero percent risk is there? No. No. Anyone who tells you that they can give you 100 percent security is either lying or
stupid or selling you something, right? Yeah, no such thing as 100 percent security. And realistically do you want to get to 95 percent? Depends. Depends. Maybe not because you might want to get to 90 that extra cost of going from 90 to 95 percent might go beyond that ceiling of that adequate risk level, right? Good. And employment of techniques and procedures for continuous monitoring of the security state. That can also be wrapped into your control. Compliance is essential to ensure that they're being followed. Compliance is based on that monitoring and using those controls to the best of your ability. So when we talk about the difference between risk management and compliance, compliance is usually an external standard that says you will do this. Risk management is hey, what is our real threat profile? What's our real risk profile? And how are we going to protect against that?
**Authorization Boundary**

**Authorization Boundary**

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

*Ref: NIST SP 800-37 Rev-1, Appendix B*

The term **information system boundary** is synonymous with **authorization boundary**.

**039 Authorization Boundary. What's the size and scope of the thing we're trying to protect? What's it look like? What's the shape of this animal? And in terms of how we look at federal information systems your information system boundary and your authorization boundary should be the same thing. You are not required, you are not responsible for securing stuff outside your boundary. That's pretty nice. That's pretty good.**
Authorization Boundary Size -1

Too Large….

- Can make the risk management process extremely unwieldy and complex

**040 If it’s too large makes it unwieldy and too complex. Anyone working on a Cloud computer off-site storage? Vendor processing? Okay if you become responsible for things that you’ve subbed out in SLAs what was the point of subbing them out?

Student: I have a question along those lines then.

Ben Malisow: Yes, ma’am?

Student: So subbing out is not giving up your responsibility for it so if I outsource and sub to somebody in India to do my call center I still have to take responsibility for that so is that still not the authorization boundary?
Ben Malisow: You are responsible for the information. You should not be responsible for the system. The responsibility for your system should be in the contract. Should be in the SLA. If it’s 99 percent up time or whatever it is, they should be the ones required to do the-

Student: Managing the out piece of it.

Ben Malisow: Yeah, yeah. Once you become in charge of something a hemisphere away, you've lost all the value of giving it to somebody who can do it cheaper. Good question. Excellent question. Ultimately as the data owner you're still in charge of the CIA of that data. Yeah, good. And if it's too small you're missing pieces. You're missing pieces. You don't want to let something go.
Authorization Boundary Size -2

Too Large….

- Can make the risk management process extremely unwieldy and complex

Too Small…

- Increases the number of information systems that must be separately managed thus unnecessarily inflating the total information security costs of the organization

**041 Anyone ever do a pen test and find broke modems or other assets that shouldn't have been there? I'm not going to dime out any of my former clients but I've been in federal agencies where we've had totally unknown wireless networks. That's creepy. That can get really spooky.
Types of Systems -1

Subsystem –

Dynamic Subsystem –

External Subsystem –

**042 Subsystem, it's just what it says it is.
Types of Systems -2

**Subsystem** – A major subdivision of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

**Dynamic Subsystem** –

**External Subsystem** –

043 A smaller part of a major information system, right? You can also look at it as a segment dynamic subsystem.

Student: Could it be like your DHDP is- because it’s changing?
Subsystem – A major subdivision of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

Dynamic Subsystem – A subsystem that is not continually present during the execution phase of an information system. Service-oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems.

External Subsystem –

**044 It’s changing all the time. It’s changing all the time. Something that’s not static. It’s not something that’s necessarily a defined constant portion of your system. It’s something you use to grab on a service basis. An external subsystem is just like it sounds. Something outside of your direct control.**
**Types of Systems -4**

**Subsystem** – A major subdivision of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

**Dynamic Subsystem** – A subsystem that is not continually present during the execution phase of an information system. Service-oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems.

**External Subsystem** – A system that would be considered outside of the direct control of the organization that owns the information system and authorizes its operation.

*Ref: NIST SP 800-39, Appendix B*

**045** That's your call center that you've subbed out that's part of your cloud computing.

Questions in any of this so far?

Student: Would you consider an external subsystem outside of the boundary?

Ben Malisow: Yes I would, I would. I would, absolutely. And again, how do you protect your data there? By contract. By contract.
More than one type of information may be contained in an information system, each of which is subject to security categorization.

An information type is a specific category of information demarcated by an organization, or by a specific law (Executive Order, directive, policy, or regulation).

Establishing an appropriate security category of an information type requires determining the potential impact for each security objective.

**046 Why do we type information? Why do we give it types?**

Student: So we know what kind of controls to put around it.

Ben Malisow: Absolutely. Welcome to the party. Outstanding. Outstanding. And these things that define them can be laws, can be legislation, could be your organizational policy, it could be a cultural imperative. Different types of information need different levels of protection need different kinds of controls, have different nature, right?
Information Types -2

System information must be protected at a level consistent with the most crucial or sensitive user information being processed, stored, or transmitted by the information system to ensure confidentiality, integrity, and availability.

This is sometimes referred to as the "high water mark."

**047 Great examples: You want to protect it to a level consistent with the most significant piece of information in that system. It’s better to secure up than type down. Know what I mean by that? Your most secure piece of information is the most secure your system should be. If you have a bunch of information, you don’t dumb down all the information so that it becomes classified at a lower level.

Student: The one place I used to work with we actually because we work it over in Switzerland, over there basically you have a lot higher data protection.

Ben Malisow: Safe harbor?
Student: Yeah, so I mean even including IP addresses was considered sensitive.

Ben Malisow: The IP is considered sensitive?

Student: Uh-hum. So we dropped that but we kept everything else.

Ben Malisow: Wow.

Student: Well not for any item outside Switzerland.

Ben Malisow: That’s pretty wild. That brings a whole new way of looking at the data then too, doesn't it? Is it expensive to run a network over there?

Student: Oh yeah.

Student: How can you put a sensitivity level on an IP address that has a public face to it, or these internally NATed addresses that wouldn't see the public? How do you stop an addressable address from-

Student: It’s actually current. It’s one of those things that just happened it’s like less than one year ago that they actually started doing this, and basically you have exactly that. This is a public facing item. What- how the heck are you guys going to be protecting this? And they basically have stated up to this point there were a couple law suits that were saying hey, you know, this is really unreasonable. It's been really a lot of problems for like the RIAA, the Recording Industry, their counterparts over in Europe to actually go after them now. It's been a major they're actually.
Ben Malisow: You would have to NAT everything, wouldn't you?

Student: Yeah.

**Examples of Information Types**

- Budget formulation
- Customer service
- Workforce planning
- Contingency planning
- Population health management and consumer safety
- Criminal apprehension
- Intelligence collection
- Intellectual property protection
- Personally Identifiable Information (PII)

*048 These are different examples of different types of information. Do all these pieces of information have different kinds of requirements on them?

Student: You're shaking your head.

Ben Malisow: Absolutely, yes they do. They do. I'm trying to mess with you. Yes, they all have different levels of information. They all have different levels
of security, different types of controls on them, right? Different laws that protect them or stipulate how you're supposed to protect them. Some of them might affect your operations in a drastic catastrophic way. Some of them might just result in lawsuits. Some of them may result in prosecution, right? Everybody familiar with all of these? Okay.

Security Controls

Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Ref: FIPS 199, Appendix A

**049 Security controls. Good definition. Again I’m not going to read it because Michael is going to throw something at me. The thing I don’t like is that they use the word inside the definition. They actually use the term to define itself, but basically it is those things that you're going to use to
protect your systems. It is the ways to obviate the threats and the risks and minimize them to an acceptable level for your organization. Are the controls all the same for every organization? No. Are they all the same for every kind of information? No. Are they all the same for every kind of system? No, of course not. So they’re all very customized. They’re all very personal to your environment, to your organization, to your information. And there’s lots of different ways to implement controls. Lots of different kinds of controls and we’ll get deep into that too.

**Classes of Security Control -1**

**Management Controls –**

**Operational Controls –**

**Technical Controls –**

**050 Three main classes of controls:**
management controls. This definition is
the fuzziest. Anyone want to take a stab at it?

Student: Over arching controls.

Ben Malisow: Yeah, usually it’s your policy. It’s your policy. It’s here’s how we’re going to do things. This is the nature of the way we’re going to do business. This is our culture’s view from an organizational perspective. It’s the risk management. It’s the management of risk. Here’s what we’re going to do.

**Classes of Security Control -2**

**Management Controls** – The security controls for an information system that focus on the **management of risk** and information system security.

**Operational Controls** –

**Technical Controls** –

**051 Operational controls? Little less fuzzy but still not as concrete as your technical. Processes, usually. Processes. People**
are often the target of operational controls.

Classes of Security Control -3

**052 Checklists, repeatable procedures, manuals, handbooks, those kinds of things are operational controls by and large. Technical controls? Easiest one. Somebody hook me up.

Student: Hardware.

Ben Malisow: It's your hardware, your software, firmware, your bits and your bytes.
Classes of Security Control -4

Management Controls – The security controls for an information system that focus on the management of risk and information system security.

Operational Controls – The security controls for an information system that are primarily implemented and executed by people.

Technical Controls – The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Ref: NIST SP 800-18, Appendix B

**053 It’s where the rubber meets the road, right? Yeah, yeah. Your firewalls, your honey pots, whatever. Good, anyone questions on those things, distinctions pretty clear? Are there some that fall into more than one category? Are there controls that overlap? Are there controls that you’re not really-- sure, sure. That’s okay too.
Notices

© 2015 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.