able to go back through other steps in the risk management process and say, "You know what? We need to relook at our controls. We need to redo our vulnerability assessment, because that seems to be out of date."

And initiate process improvement activities-- the idea that you're going to do some type of gap analysis here and see: "We have problems. How do we improve that? How do we fix that?" All of that happens here in the risk monitoring.

NIST SP 800-39: Risk Response

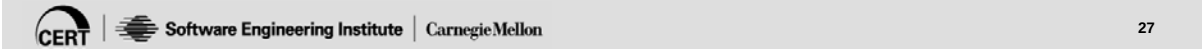
When organizations experience a breach/compromise to their information systems or environments of operation that require an immediate response to address the incident and reduce additional risk that results from the event

The risk response step can receive inputs from the risk framing step.

- When is the organization required to deploy new safeguards and countermeasures in their information systems based on security requirements in new legislation or OMB policies
- Shapes the resource constraints associated with selecting an appropriate course of action

The risk response step can receive inputs from the risk monitoring step.

Ref: NIST SP 800-39, Managing Information Security Risk



**027 With risk response, this is what you do when you actually have an issue, like a security breach. You go into incident response, or whatever your processes might be there.

For risk response, generally you're going to be taking inputs from the other aspects, from the assessment, from the monitoring, and even from the framing step within that particular section. And because of that response-- you get inputs from the framing section or the framing process, risk framing process-- you're able to better select the course of

action that you want to do, pick out, "Here are the steps that we need to take in terms of risk response."

NIST SP 800-37

NIST SP 800-37

Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

Guidelines developed to ensure that

- Managing information system security risks is **consistent** with the organization's **objectives and overall risk strategy**
- Information security requirements are **integrated** into the organization's enterprise architecture and SDLC

CERT | Software Engineering Institute | Carnegie Mellon 28

**028 800-37, another publication. This presents the security lifecycle, or how do we address security within our organization. It does give you some guidance on making sure that your risks are consistent with your risk appetite or your organizational desire for managing risk. So it's kind of balancing risk and what our business actually wants. And it makes sure that your requirements-- so, as your-- or your requirements are integrated into some type of

lifecycle. Meaning, when you go out and you purchase a new system, or you bring in a new application, when should you start thinking about the security of that application or system? Before you buy it, after you've bought it, or after you've implemented it?

Students: Before you buy it.

Chris Evans: Before you buy it. Now, when do people usually get to thinking about security?

Student: Once they have it in-house.

Chris Evans: Once they have it in-house, once the lights are blinking and everybody goes, "Ooh, that's great., We like it." Okay, what about the security of it?

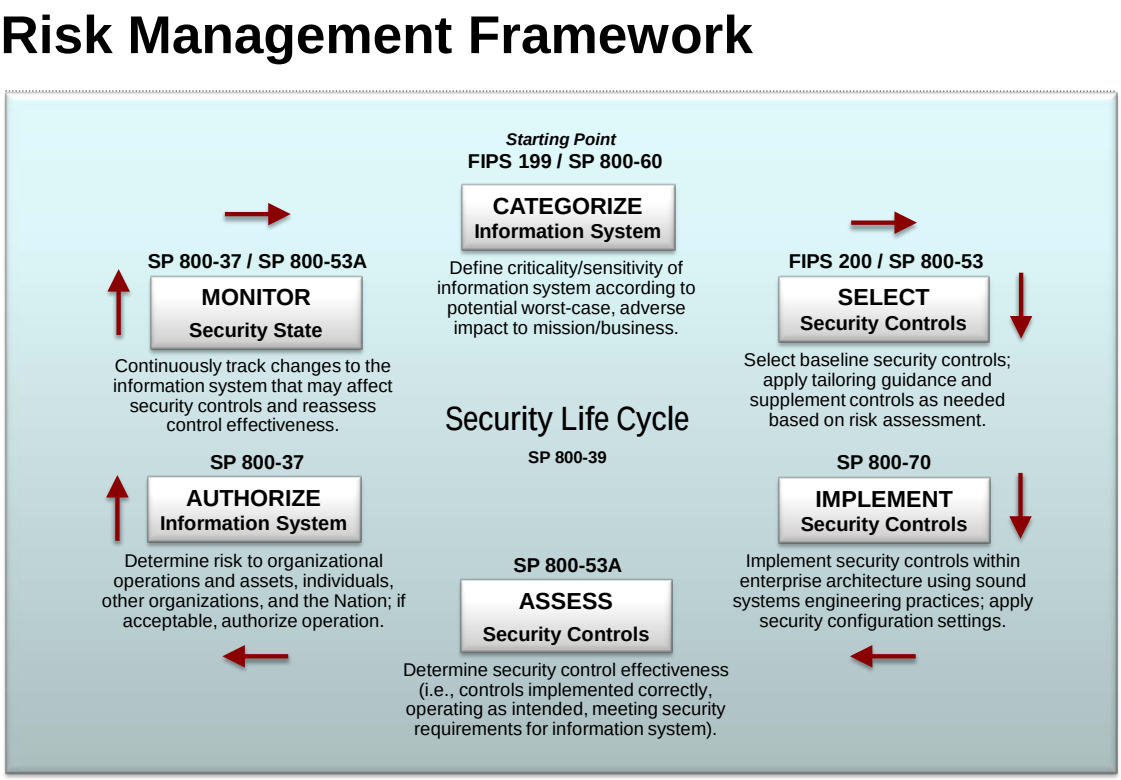
So there was an example of an organization who brought in a nice little Polycom system, one of those teleconference systems, and in the documentation for it, the Polycom says, "You have to put this outside your firewall. And oh, by the way-- warning, warning-- it opens you up to attacks," and yada, yada. I mean, it's all documented in there. So, good disclosure from the manufacturer on this device. Right?

So somebody said, "Okay"-- somebody within the business unit said, "I want the Polycom. I want it here, because I need to do business, and oh, by the way, I needed it yesterday. So go buy it, put it in,

and we'll be all right." Three hundred thousand dollars later, the Polycom comes in, is sitting on the table, and the people go, "Oh yeah, we need to talk to security about this." So it's already up and running, it's already connected in, and the security guys come over and go, "Oh. Well, this is going to introduce all sorts of problems." Now you have security versus convenience. Right? "Well, I have to have the Polycom to do business, but the security guys are telling me this is a terrible thing to have because it opens up our network to attack." Well, now what do we do? What do you think is going to happen? The organization already spent 300 grand on the Polycom device.

Student: Risk assessment.

Chris Evans: That's what hopefully happens, but usually what happens is the Polycom stays there and the security guys are left to figure out how to deal with it and how to mitigate that.



**029 So, you look at the security lifecycle that's presented here. Kind of in the-- this is the lifecycle that comes out of 800-37. Right in the middle of this thing you have the overall guidance. That comes out of 800-39. You're going to start your process up at the top of this chart.

So, up at the top there, we have categorizing information systems. So, we've talked a lot about risk management. What's the first thing you do? Identify your critical assets. Right? Systems, people, that sort of thing. So you're categorizing your information systems. You can get guidance on that out of FIPS 199 or

800-30. Both of those-- or, sorry, 800-60. Both of those documents will help you categorize your information system.

Once you do that, you're coming over here, and you're going to look at the security controls that you want to put in place to address the risks. You can look at FIPS 200 or Special Pub 800-53. 800-53 is a thick document and it lists hundreds of controls that you can put in place, separated by different functional areas. So, when you're selecting security controls, take a look at 800-53. There's a bunch of information in there for you.

When you're implementing security controls, take a look at 800-70. This has checklist guidance in it, and will help you determine how to implement security controls within your organization. Once you've got it implemented, you're going to start looking at assessing it. How do the controls work? Do they work as intended? Are they really what we need? So, take a look at 800-53A. There's a reason it's 53A, because I said a few minutes ago that 800-53 lists all the controls that you could implement. Well, a significant majority of them, right? 53A is the companion document to that, and 53A tells you how do you assess each of those controls. So 53A will list-- or, sorry, 53 will list what the controls are; 53A will say, "For each of those controls, here's how you assess the effectiveness of that."

Once you've assessed it and you've said, "Okay, we're ready to put this system into practice," you can authorize it. So, the certification and authorization process is governed by 800-37. And then monitoring. You do continuous monitoring on this to make sure that things-- if things changed, your controls are still effective and still work. And so you monitor that. You can take a look at 53A-- again, that's the assessment piece that we talked about down here at the bottom of the diagram-- and 800-37. Both of those documents will kind of give you guidance on how to do this.

So this kind of eye candy chart right here tells you the documents and the guidance that's available to you, at least from NIST and the U.S. federal government on risk management.

Notices