NIST SP 800-37 Risk Management Framework

Table of Contents

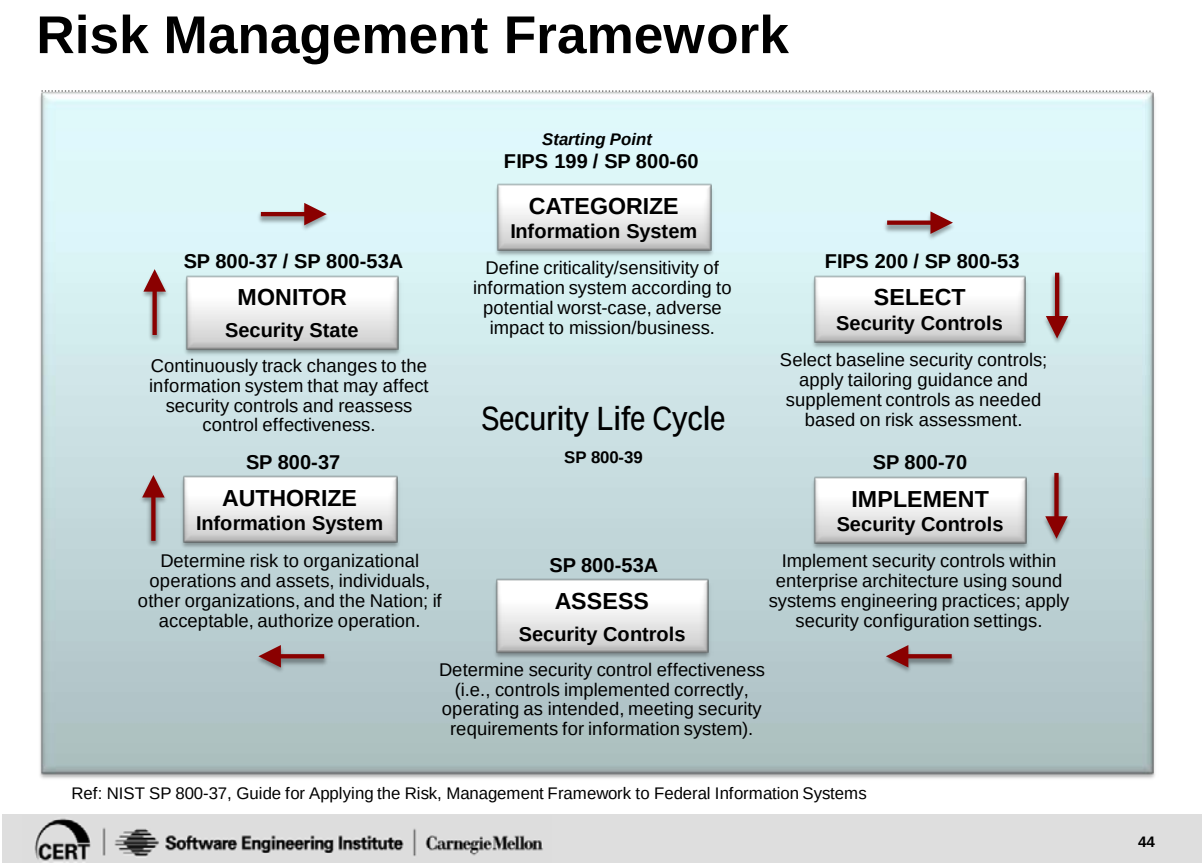
NIST SP 800-37

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

**043 So the other one here, we have 800-37. Again, this prescribes kind of a risk management framework, or how to apply risk management framework from a lifecycle perspective. Really, it kind of comes through and makes sure that your risk management process is ingrained within your organization; it's at least consistent with what you do; you've adopted it and it's now part of your change management process, your continuous improvement process, or even your lifecycle processes. So 800-37 will help you figure out how your risk management plan fits into your organization and makes sure it stays there.



**044 This is a great chart, because this shows you all the NIST Special Publications and where they fit into the risk management process. And so if you look up-- excuse me-- at the top here, where we're categorizing information systems, remember we said earlier you have to have a good understanding of what your assets are, whether the data on it is critical, data on it is sensitive or not. So you start by categorizing your information systems, and if you look at Special Publication 800-60, or FIPS 199, both of those documents will help you categorizing information systems, understanding what's critical. Yes, sir?

Student: Where does 800-30 fit in there? I don't see it up there.

Chris Evans: 800-30-- you're right; it is not up here. So 800-30 describes the risk management process overall. So this is the lifecycle, and this is described by 800-39. So 800-30 is kind of an umbrella policy-- or, sorry-- umbrella standard over all of this.

Student: What's the numerical convention for NIST? So, obviously 800-30 series is risk, or is there an index for that? So you have dash-70 there. We have 53-60, 53-837.

Chris Evans: Because within this process, you look at--

Student: Seems kind of random to me. There must be some kind of--

Chris Evans: Kind of. I mean, you can say that the 30-level publications are kind of high level, and as you go into deeper technical detail, it's the 53. But there are no other 50-series publications.

So we'll move over here to selecting security controls. So if you're trying to figure out what controls could I put in place and how do I know whether that control will work or not, you can look at FIPS 200 which will tell you, "These are the ones you must have," or you can look at 800-53, which is an encyclopedia of controls. And there are hundreds in there, that gives you guidance and instructions on how to implement

those, or at least what those controls are. Because 800-70 will tell you how to implement those controls that you've looked at up here. 53A is kind of a sister publication to 800-53. If 800-53 is all the controls that you can implement, 53A tells you how to assess all those controls that are in there. So 800-53 and 53A are thick documents.

800-37. If you have requirements for certification and authorization, C&A process, 800-37 will help you through that and understand what the components are there. And then 800-37 and, again, 53A, will help you monitor: Do my security controls work? Are they being effective? And how do I integrate changes, configuration changes, that sort of stuff, into a process where my risk management doesn't get outdated?

Notices