Risk Management Overview

Table of Contents

Risk Management Overview

Risk Management Overview

5

**005 Instructor: This is the risk management overview.

Risk Management

- NIST SP 800-30
  - Defines **risk** as “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence”
- At a high level, this is accomplished by balancing exposure to risks against cost of mitigation and implementing appropriate countermeasures/controls.

CISA CYBER+INFRASTRUCTURE

6

**006 Let's start by level-setting with how we actually define risk. Now, I always start with the fact that risk is uncertainty. No matter what, if you hear the word risk, you should automatically start thinking of something I don't have certainty around. So there's going to be a likelihood issue that's going to be associated here, like a probability, if you will.

Now, any good risk is going to have a couple other elements. One is it has to have a threat actor or a source. Now by the way, that threat actor or source may be knowing-- they may be malicious-- or maybe not. It may be a risk or uncertainty based upon ignorance.

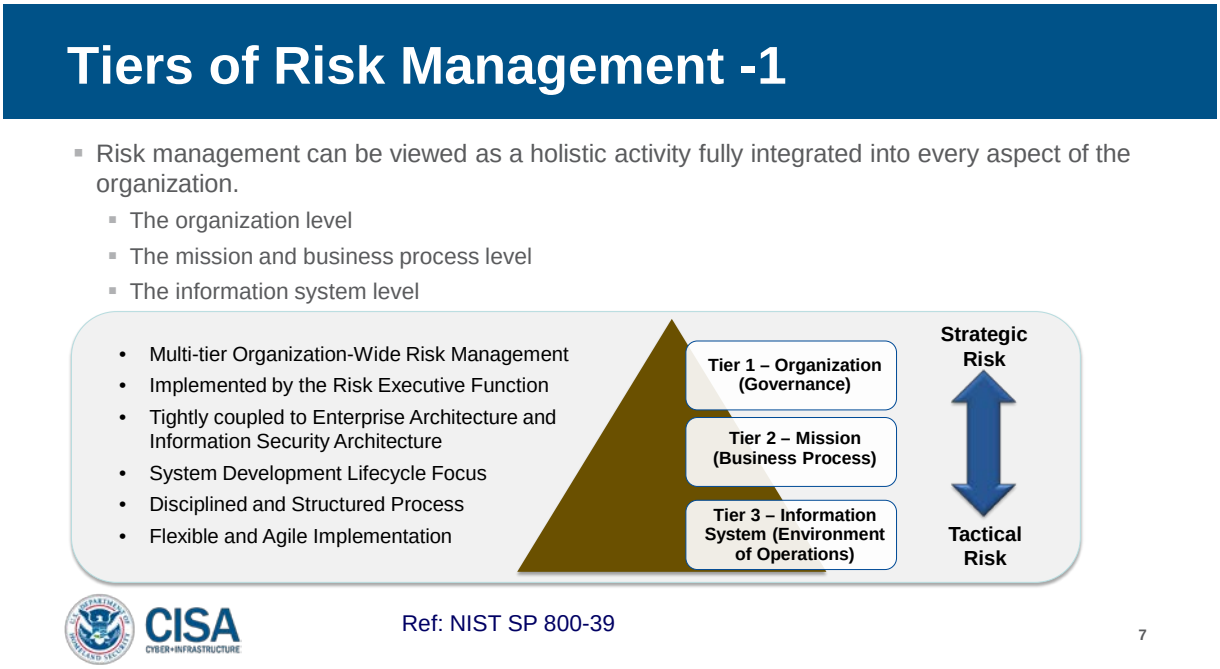
Also, you're going to have to have an asset that has a vulnerability to it.

This is some gap, a chink within the armor, if you will, that that threat source is going to be able to tap and get in your system and/or your organization, and actually inflict some kind of action that brings about impact.

Now, I like to actually start here by level-setting the idea too that a risk does not necessarily have to be negative. We always talk about risk, and it's kind of a red word. People get tense when they hear about this. But the impact could necessarily be a positive one. So let's say I'm making a sale. There's uncertainty around making a sale. But that said, the outcome could be very positive for both the salesperson and the person who wants the product.

So we can treat risk as two sides of a coin. One is the risk could be a negative event. It could have a negative or adverse impact. Or it could be a positive one, where you have a positive impact for the organization. So at a high level what we're trying to do is we want to get to a point where we've invested enough time, planning, possibly even resources to either maximize the ability to realize a risk, if it's an opportunity, or we want to limit it ever happening.

Tiers of Risk Management -1



**007 There are different ways to think about this too. Just because we have a risk doesn't mean that just the person at the front lines is the one that's feeling it. There's NIST SP 800-39. I recommend going to read that document.

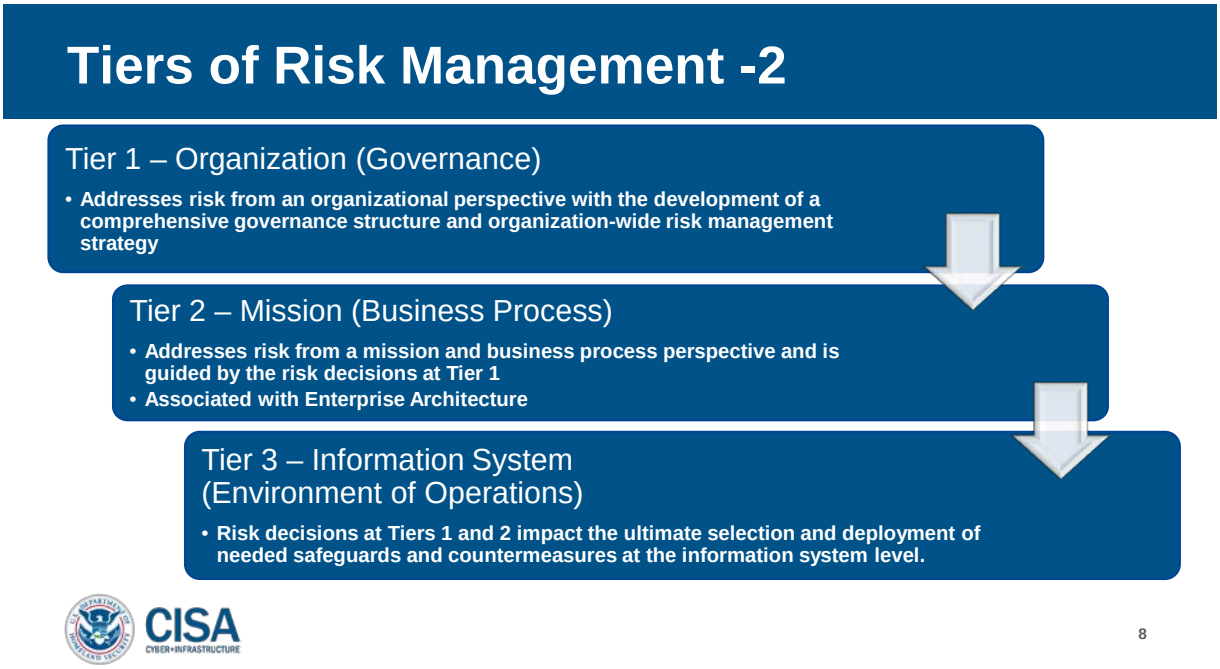
NIST actually sees risk laid out in an organization, and they do a really good job at talking about tiers.

So you want to think about risk happening across an organization, from top to bottom, and you could think about risk in the long-term, and these are like the big, enterprise-type risks, and those are strategic, and they're really handled usually at the top of an organization, where you have an upper-level governance, right? And then maybe you start talking about missions within that

organization and you talk about business processes to realize those missions, and there are risks at that level too.

And then at the bottom, at the front line, you're going to actually have a third tier where you're going to actually have an environment where these operations take place, where these missions have to be accomplished, and that's where you're getting now down more to tactical risk. So this could be things way down in the weeds, if you will. Maybe not as strategic, and maybe there's a possibility they could be realized more often, but in that case, maybe the impact is less. It all depends on the type of risk and the analysis.

Tiers of Risk Management -2



**008 So we're going to start talking a little bit more about that in

terms of how these risks can actually somewhat amalgamate, especially if you have them at the lower level of the organization, in that environment, if you will. Now this is the thought that risk could actually turn into the death by a thousand cuts kind of an idea. So you have to manage risk at the tactical level just as much as at the strategic, because you could run into troubles here where you ignore risks at the lower levels and they all sort of build up on you and they'll start realizing failure of mission, and you have a real bad day, you actually have missions that fail and your organization starts faltering. So we want to think about risk in terms of how big it can be in order of magnitude of impact, but you also want to think about how profound it would be at different levels of this map that I'm giving you here in terms of tiers.

Terms to Know Related to Risk Management

Terms to Know

Related to Risk Management

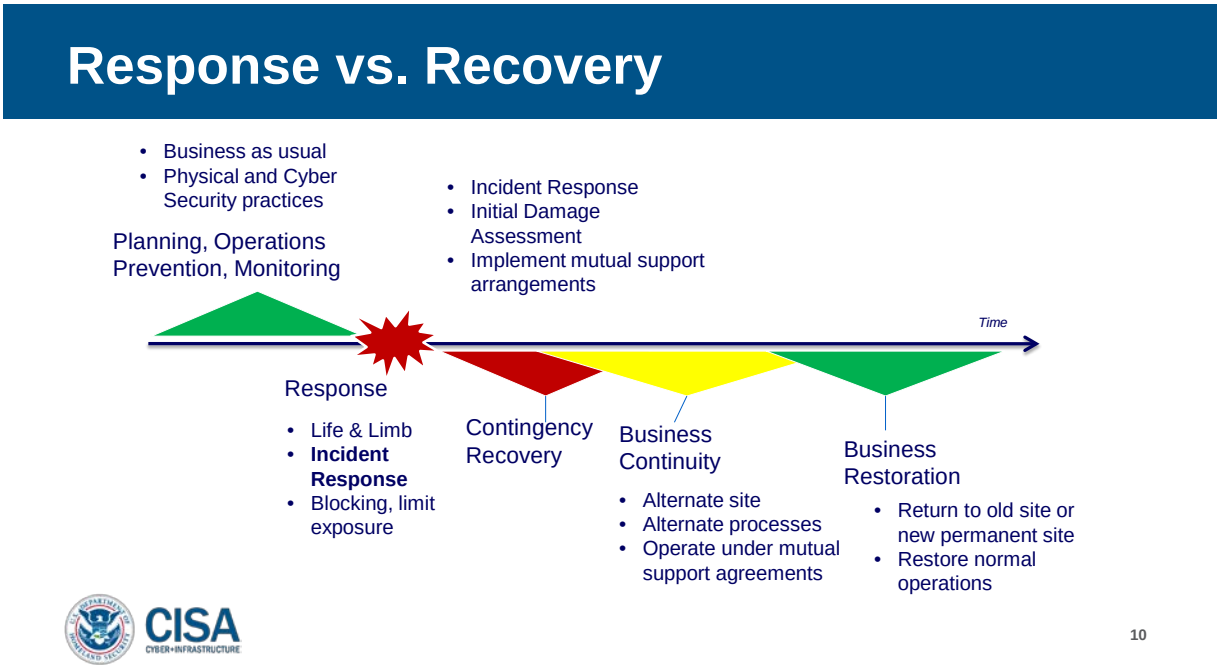
- Response vs. Recovery
- Threat, Vulnerability, and Risk
- Risk Assessment
- Business Continuity Management
  - Risk Assessment
  - Business Impact Analysis (BIA)
  - Business Continuity Planning (BCP)

CISA
CYBER+INFRASTRUCTURE

9

**009 So we're going to go over these terms. We're going to talk a little bit about response and recovery, some threat and vulnerability, risk assessment--basically the meat and potatoes to risk management.

Response vs. Recovery



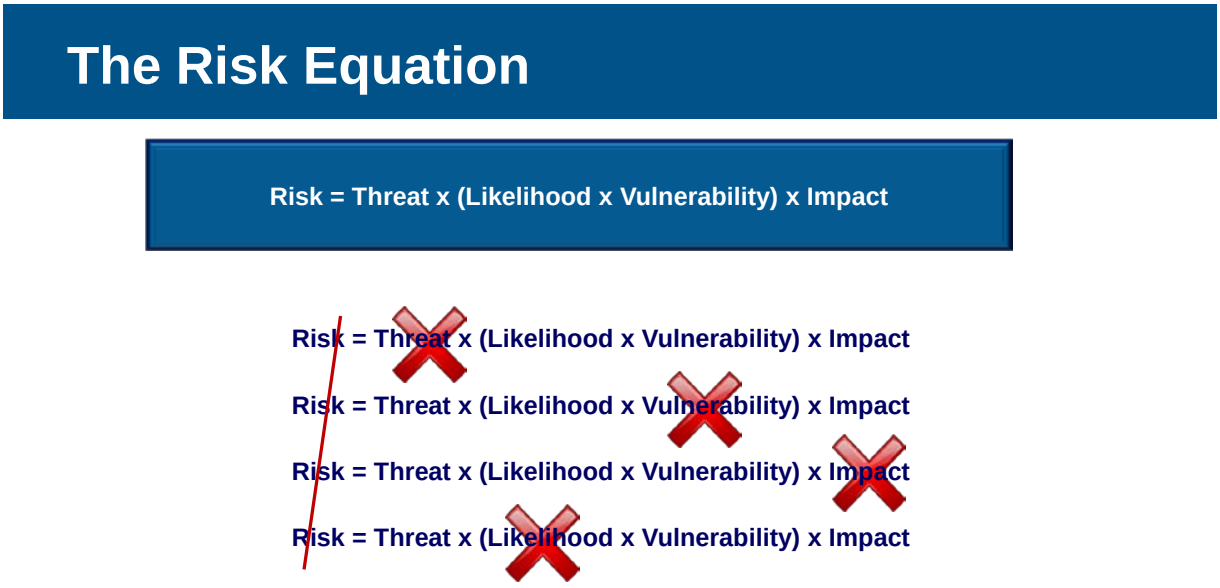
**010 Let's first start with response and recovery. So, there's this notion that a risk has a lifecycle to it, and I'm somewhat jumping the gun here. I'm going to get to risk in the end and we're going to wrap this up, but what I wanted to start with is this idea that there's a timeline for risks as they come to fruition.

If you think about it, there's a before-the-risk-ever-happens type time, where you're actually planning; you're trying to prevent; you're doing all the right things. It may be perceived as business as usual. Maybe there's special projects that you have set up to avoid these risks. Maybe there are things that you're doing in your security operations centers-- we'll talk about that at a point in this overview-- but there's going to actually be that day where

that risk will actually come to fruition. It will happen, and you're going to have to have a response to that risk, so that's right at that point, and it's very tactical. It's going to happen very much at that moment. You're worried about saving life and limb. You're worried about instant response, and hopefully immediate actions that you can take to limit the impact that's going to take place there at that point and following.

And then you're going to enter this latter period of time after the response period where you're actually recovering your original operations, and this is going to start talking to terms-- you'll hear me say things like business continuity, restoration, returning to normal operations. So as long as you keep that map in your head, response and recovery shouldn't be an issue.

The Risk Equation



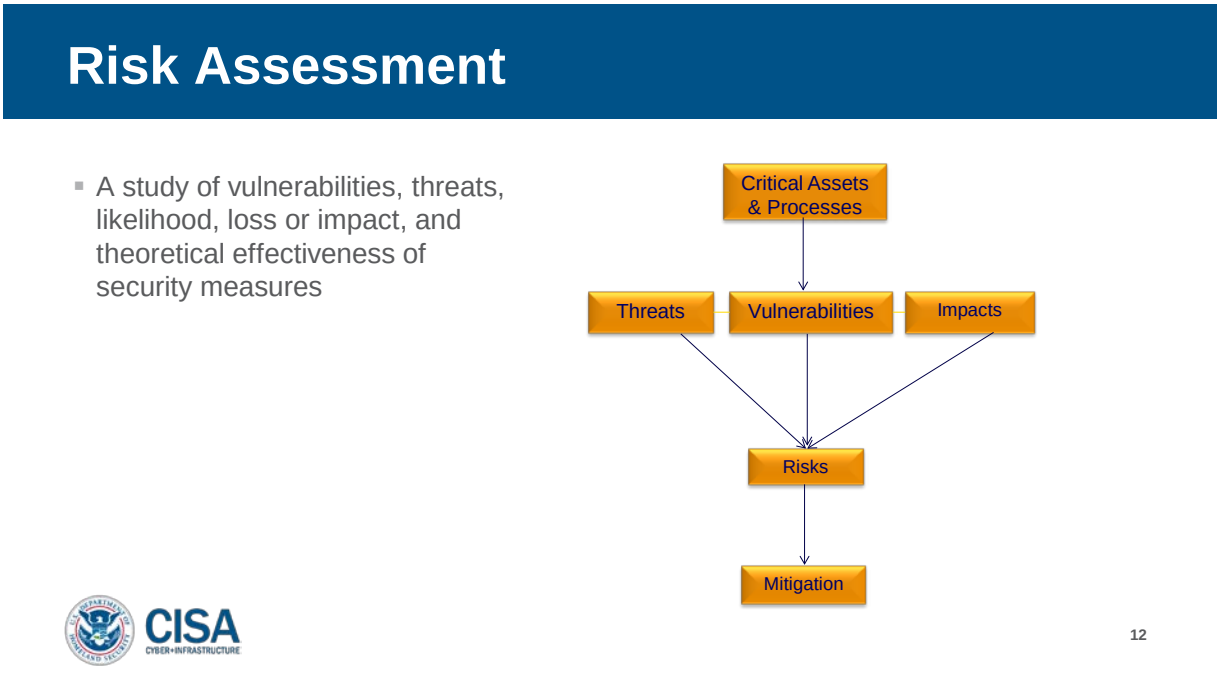
**011 Now, any good risk, as I had said before, has three distinct elements to it-- actually four if you're looking at this-- but I like to think about it in terms of the threat, the vulnerability, and the impact, and in the meantime, we're going to talk about that vulnerability. There's maybe a likelihood that's associated with it actually being taken advantage of. But what I want you to walk away with for this particular slide is I can control risk by taking out any of these elements from the risk equation.

So if I eliminate the threat-- so if you imagine my critical asset being a castle, and I have a wall around that castle-- that would be maybe my control set-- and the risk is the idea of the wolves outside the gate getting into my castle, or getting to

that critical asset. If I eliminate the wolves, then I no longer have a risk. So I've eliminated that threat, if you will.

I could eliminate vulnerabilities. Maybe that wall has gates. Maybe if I close all the gates, I've eliminated the fact that there's any vulnerability for any way for those wolves to get into the system. Also I could eliminate the impact. I could actually say, "Hey, that castle means nothing to me," and walk away from it, and once again, the risk doesn't exist. Or I can do things to try to limit the likelihood, to bring it down to a level where that risk no longer would have any meaning in my portfolio.

Risk Assessment

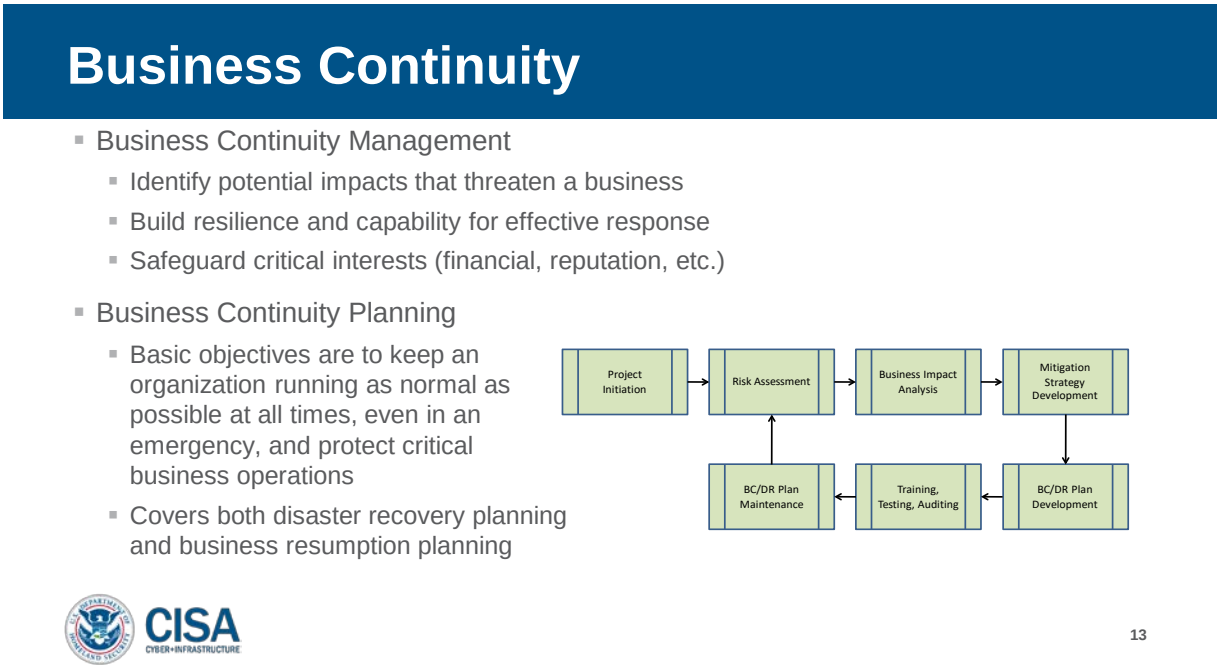


**012 So we're going to talk about how we respond to that as well in the future here and how you can affect

each of those elements over the course of this discussion.

So now I've given you this analogy, this castle and these walls, and we have to understand how we go about analyzing it. How does the king know that the castle is going to be protected? Well, first you have to really get in touch and understand what are your critical assets and processes? What are you relying upon? It may not necessarily be the castle itself. Maybe it's the crown jewels within. It may be the people that you're protecting. It may be a process. Maybe it's a mission. Maybe you have gardens that are feeding your people within and you don't want them to be damaged. So you're going to have processes related to it you're going to want to address in terms of maybe, say, growing your crops, right?

You also have these threats I talked about-- the wolves, right? And they can inflict impacts on your organizations and they're going to try and get into that by exploiting the vulnerabilities that you have, and this all amounts to risk, and what we need to do is we need to mitigate this, as I've been talking about.



**013 So let's go back to that recovery-response piece, because now what we've done is we've understood the uncertainty related to this specific event that may take place, and now we've gone through the fact that this risk has come to fruition, and we've gone through the response, and now we're worried about business continuity.

So let's say the wolves get in, we respond, we eliminate the problem-- maybe, I don't know, we give the wolves a nice bit of kibble and they're happy and maybe they go away. That's one response, right? But now we're worried about getting back to our normal operations-- normal course of operations.

Now, there's a lot of up-front planning that comes with business

continuity, and I think this is where a lot of organizations maybe come up short, because it takes time, and it takes money, and what you need to do is actually make a meaningful effort around managing your business continuity and actually planning for it when that dark day has come and passed and now you have to recover your operations. So you want to ask some critical questions here: What are critical impacts that could happen to my organization that would actually make it so my organization couldn't operate? How is it that I would build a resiliency capability so that way I can bounce back, if you will, as quickly as possible? And how would I maybe safeguard these critical interests maybe such that they're not impacting at all?

And you also want to think about too: What are the objectives of the organization? So at the base of it, at the very start, what you really want to do is get back to: What is it that your organization is trying to deliver? Truly, in a lot of cases, you may run into some surprises here. If you were to go around and ask everybody in your organization what it is they're trying to truly contribute to the organization in meeting objectives, it will really put into perspective how critical their function is in terms of what they need to achieve and where they might fit into this business continuity plan.

**014 So with that, you may want to do what's called a business impact analysis. So you have to determine what is important to you, and remember I mentioned the critical assets idea. Now this all dials back to not just what are critical assets, but what are the critical services, what are the functions that your organization delivers, and you have to know what are the threats to that. Now, in this example I said wolves. I mean, it could be anything. Maybe it's a bunch of brigands and they want all your goal, right? That kind of a thing. So you got to really think about what it is that you have that's critical.

In any cyber organization, it's information maybe. So you want to think about what people want from that information. You want to think

about maybe the idea that they want to interrupt your operations. Maybe it's the fact that they have ransomware and they want to just shut down your operation and they're just using ransomware as some kind of ploy. They really want to just shut you down and they really don't even really want anything that you have, per se. They just want to slow your business down. So you have to think about threats, and you want to think about the motivations that they have there.

You want to dial back too and you want to think about, "Okay, so now I understand what my assets are. What are the vulnerabilities, and what's the likelihood that those vulnerabilities may get exploited?" Now this becomes a very challenging piece of the puzzle. If you think about it, Microsoft-- they do updates to their software all the time, trying to close gaps where they've identified vulnerabilities, and new ones exist, time and again. Some exist out there-- and we're going to talk about advance persistent threats-- where advanced persistent threats will identify a vulnerability before anyone else understands what they are, and you could be caught by surprise with them. So we're going to have to really get out hands wrapped around what vulnerabilities are to our assets if we really want to control this risk issue.

Types of Risk

- **Inherent Risk** is the risk linked to a particular activity itself.
  - Complex regulations
  - Poor management
- **Control Risk** comes from a failure of the controls to properly mitigate risk.
  - Failure of firewall to block malicious traffic

- **Residual Risk** is the combination of the inherent and the control risk; it is what remains after the controls have been applied to mitigate risk.
  - Eliminating risk is not possible IF you have chosen to expose yourself to it.
  - Residual risk must be accepted by management.

CISA CYBER+INFRASTRUCTURE

15

**015 So there are different types of risk, and really a risk, like I said, is an uncertainty, unlike anything else, but what I really want to cover here is the idea that sometimes you'll hear these other terms. So I felt it's important that you understand at least what they are if you hear the words.

So I'm going to go out and I'm going to conduct operations, and no matter what it's unavoidable that I'm going to have risk related to operation, and that's inherent risk. I have some examples. It could be a matter of I'm engaging in some operations where there are complex regulations. Maybe I have poor management of the operation itself, and if that's the case-- I get it-- then there's going to be some risk related to that process.

There may be control risk. Now this is an interesting one, because this is actually saying that I've actually taken action to mitigate my risk, to actually keep it from happening, or maybe at that cold, dark day, to limit the impact. But there may be some risks that I inject into the process that would actually make it less appealing in terms of how effective that control is. Those are control risks that I enter into there.

And then there's this idea of residual risk. So I have that inherent risk around an operation, and suppose no matter what I do, no matter what controls I set up, there's still some element of risk that's going to remain. That's residual risk.

Operational Resilience

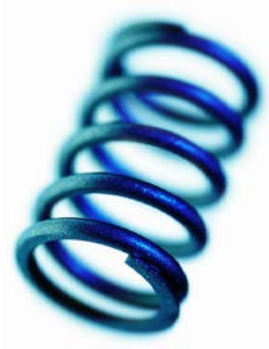
Operational Resilience

- **Resilience:** The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit

  [wordnet.princeton.edu]

- **Operational resilience:** The *emergent* property of an *organization* that can *continue to carry out its mission* in the presence of *operational stress* and *disruption* that *does not exceed* its limit

  [CERT-RMM]



Where does the *stress* and *disruption* come from? RISK

CISA CYBER+INFRASTRUCTURE

16

**016 So ultimately, what are we trying to get to here? If I understand

risk and I'm able to control it, really what I want to do is I want to make a more resilient operation. I want to make it so that no matter what happens, no matter if all the gates fell down, no matter what, I can still carry on with business. This is resiliency, in a nutshell.

Now, there's this classic question of the chicken and the egg. What comes first, a resilient enterprise, or an enterprise that understands risk really well? In my mind as I go through it, you really have to manage risk really well before you can really have any bit of assurance to understand that you have a resilient operation.

So you might want to think about resilience one more way, and there's a picture here of a spring. I know when I was a kid, I had Slinkys, and my brother always destroyed it. But before he'd destroy it, you'd stretch it out and you'd let it bounce back, and it would recover. So think about that as your operations. No matter how much stress I put on it, it's able to return to its normal form. But then that brother comes along, he trashes it, he was the threat actor, and it can no longer get back to where it needs to be. So that in a sense was a risk that came to fruition and it wrecked my ability to be resilient with that toy. So we want to think about this in terms of controlling risk to be more resilient.

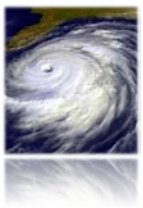
Operational Resilience and Risk

- ***Operational resilience*** emerges from effective ***operational risk management.***
- Operational risk categories

Actions of people

Systems and technology failures

Failed internal processes



External events

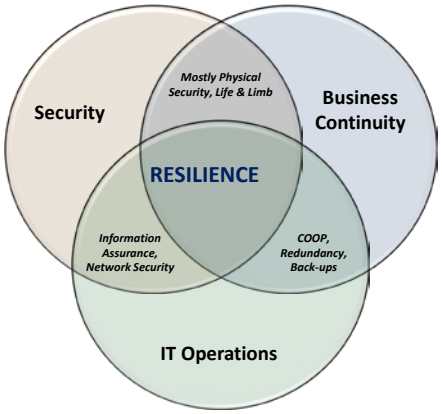
CISA CYBER+INFRASTRUCTURE

17

**017 And there's different ways the SEI thinks about this. I'm going to refer to a document and a model that we have called RMM, and what we want to think about with this operational resilience and the way we have it set up in RMM is we think about how people take action. We want to think about how systems may fail. We want to think about the processes that we have set up. Or it may be a broader force majeure event that happens outside the organization.

Elements of Resilience …

- You should focus on all three; do not ignore one for the others.



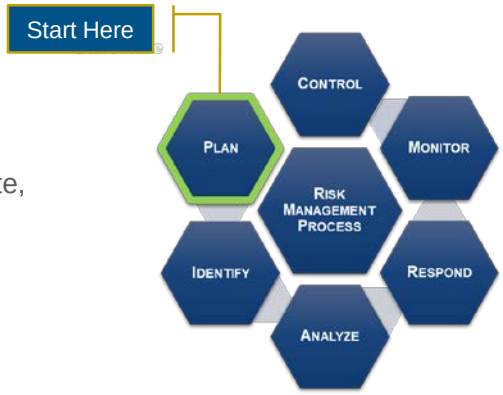
CISA CYBER+INFRASTRUCTURE

18

**018 There's some elements to this resilience that we need to think about too. It may be the idea that we have security in our enterprise. We may have thought about the business continuity elements. We may have operations that are taking place at all times, whether they're IT operations or otherwise. And there's truly this Venn diagram here of overlap within these. It's important to be familiar with where these elements are overlapping, so that way when you're developing your plans to remain more resilient, you know how in fact they are impacting each other, influencing each other.

Risk Management in a Nutshell

- Identify assets, threats, and vulnerabilities
- Determine “likely” threat scenarios
- Create and implement an appropriate response to reduce exposure
- Continually monitor, review, assess, evaluate, and update



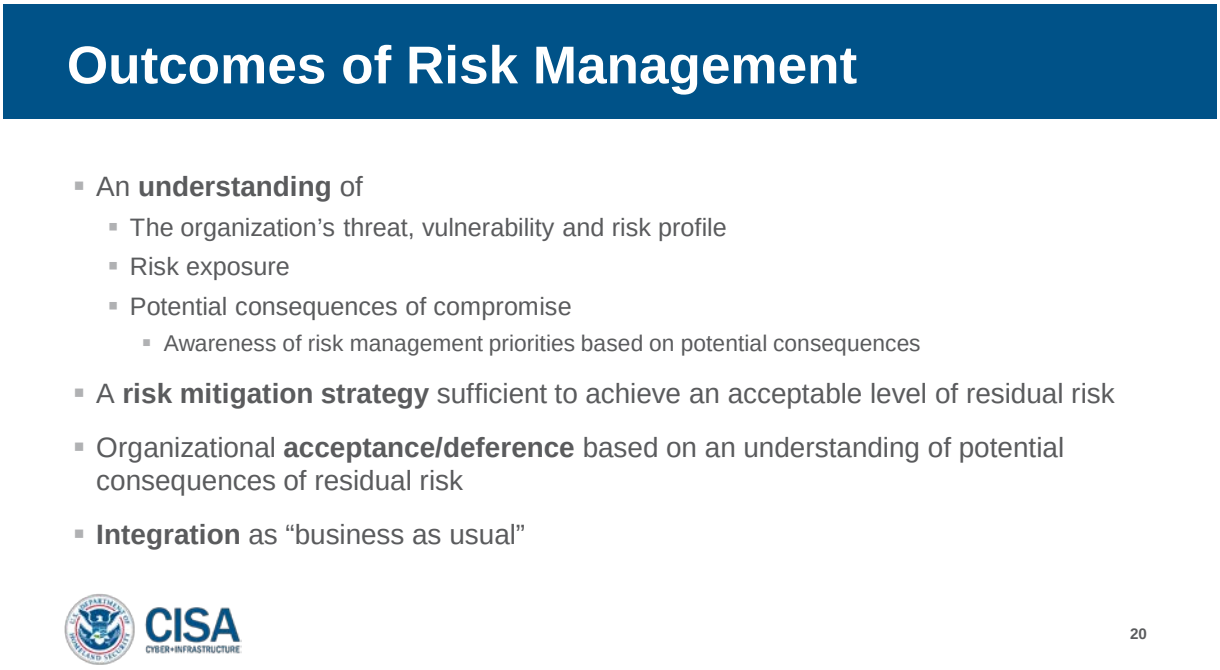
CISA CYBER+INFRASTRUCTURE

19

**019 So to wrap it up, risk management is a process like any other, and if we start at the planning phase, like we had talked at the very beginning of this presentation, and we go through and we identify what the risks are-- first of all, let's not just identify the risks. Remember that we identify the assets too, the critical services that lead you to the critical assets, and we understand the uncertainties related to them. We analyze them and understand what risks are more important. Maybe there's a prioritization there that needs to take place. We have to understand how to respond to those risks. What is it that we're going to do? Are we going to avoid altogether? Are we going to accept the risk and just let it happen? Are we going to try to mitigate it?

Whatever plan we decide to embark upon there, we going to have to monitor and see if that risk is ever going to happen. Maybe there are immediate actions we need to take if the risk does come to fruition. That's the monitoring part. And we're ultimately controlling that risk time and again. So we're going to iteratively come back to that risk and make sure we're doing the things that we need to do to keep that risk under control.

Outcomes of Risk Management



**020 So what we're looking for here is that our organization can control threats, vulnerabilities, and/or also the idea of controlling the idea threat any of these threats and vulnerabilities could impact the enterprise in a negative light. We want to limit that exposure. And it's a balance, because we could invest a

lot of resources into keeping that balance, but at the same time we don't want to build a 100-thousand-dollar fence around a stack of pennies. So we're going to talk about how we can actually analyze these risks properly so that way we can control that amount of spend, and that all goes to establishing a risk mitigation strategy so that we have an acceptable level of risk; and eventually what we want to do is get it to a point where we've got this risk management process at a state where it's business as usual. We have professionals at the front line who are constantly identifying new areas of risk and they bring it to a governance structure and we manage it in a systematic process.

Scenario A Department of Defense Example

Scenario

A Department of Defense Example

- Naval Battlegroup Deployment:
  - Consider the battlegroup your “Tier 1”.
  - Then identify your mission(s) “Tier 2”.
- At Tier 1, you have to think about big picture strategy:
  - Power Projection
  - Win Wars
  - Adversaries
- At Tier 2, you have to think about mission objectives:
  - Deploy to a region
  - Conduct maritime interdiction operations
  - Conduct anti-submarine warfare operations
  - Train with a foreign allied force

CISA CYBER+INFRASTRUCTURE

21

**021 Let's assume we have a Navy battle group, and we want to look at the

different tiers, as we talked about at the beginning of the presentation. So the battle group itself will be the first tier, and then we have missions within that battle group. So we have all these assets-- maybe a carrier, maybe we have some cruisers and some destroyers around it, maybe a couple submarines, all the associated aircraft-- and they're all executing missions, right? So you have to think about that big-picture strategy at that tier one, right? We want to project power. We want to win wars, if there are any. We want to control our adversaries, right? But within that, we're also going to have mission objectives, right? So we're going to deploy to a certain region. Maybe we have freedom of navigation operations somewhere in there. Maybe we have some kind of interdiction operations that would take place. Maybe we're beating up on the pirates and making sure that they don't exploit merchant fleets, things like that. These are individual missions that take place.

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, 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. 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.

DM18-0098