Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 23

Alright, so we have been talking about this, the resilience review, and we said that the resilience review is based on 10 domains of, you know, cyber security that need to be taken care of by the organization in order to be resilient. As I said, resilience is the property of getting back to normalcy after a cyber crisis or after some kind of a cyber incident, and your ability to do that as quickly as possible is kind of the measure of your resiliency. The question is, of course, one could argue that we should do this, that, and the other in order to be considered resilient. In fact, right now, as we speak, in the Bureau of Indian Standards, we are working on a resilience standard, right? There has been a lot written about resilience in the literature, in various organizations such as NIST and Homeland Security, and so on. Still, resilience, the term, is often misunderstood, and often people confuse it with reliability. Reliability is about your ability to work, you know, when there is a planned incident.

CRR Domains

Table 1: CRR Domain Composition

CRR Domain	No. of Goals	No. of Goal Practices	No. of MIL* Practices
Asset Management	7	30	13
Controls Management	4	16	13
Configuration and Change Management	3	23	13
Vulnerability Management	4	15	13
Incident Management	5	23	13
Service Continuity Management	4	16	13
Risk Management	5	13	13
External Dependencies Management	5	14	13
Training and Awareness	2	11	13
Situational Awareness	3	8	13

* Maturity Indicator Level

Each domain is composed of a purpose statement, a set of specific goals and associated practice questions unique to the domain, and a standard set of Maturity Indicator Level (MIL) questions.

So, when we design a system to be reliable, we already know what can go wrong and accordingly, we figure out the probability that my system will not work or will fail to provide the service in the face of those problems that I might have already imagined or

modeled. Based on that probability, we say this is the reliability. For example, we often require that you have to have 4-9s reliability, which means that it has to be 99.9999 percent probability that it will work irrespective of certain problems.

Resilience, on the other hand, is for unplanned, unexpected situations. The question that one has to ask is, under unexpected, unplanned circumstances, can we actually remain in service, maybe in a reduced capacity or reduced quality of service, but still be able to recover as soon as this problem goes away?

Then, the question, of course, is, as a cyber security team or the party responsible for the cyber security of an organization, what should be done for the organization to be cyber resilient, right? According to this RMM, the Resilient Maturity Model, they decided that there are 10 different domains in which we will have certain goals, right? These goals, if fulfilled completely, must be checked to see whether they are being fulfilled in a planned way or an unplanned way, whether the fulfillment is ad hoc or under the support of management, and whether the methods for fulfilling the goals are being reviewed to see if they are actually being met. This kind of stuff. Based on these factors, we define the maturity level.

We will see very soon what that means. Here you see that we have four columns, and in these four columns, this is the number of goals. So, per domain, I want to—I have, or their model has—this many goals in each of these cases, and the number of practices associated with each goal. Like last time, in the class, we actually looked at some of the goals—one goal, at least, for asset management. The goal was that the services are identified; that is, the organization is providing some service or set of services, or it has certain services that are externally facing, customer-facing, and certain services that are internally facing. For each of these services, I have to identify the assets associated with the service. So, that was one of the goals in asset management that we looked at.

We then saw the questions associated with each of these goals. We looked at a couple of questions. We will go into a little more detail today, but there are 30 practice questions across these 7 goals, like "Do you do this?" or "Do you do that?"—this kind of stuff. Then there are 13 what we call maturity indicator level practices—MIL stands for maturity indicator level. Each of these has 13 maturity indicator level practices, and they are actually the same set of questions for each of the domains. So, we will look at that.

The domains that we are interested in include asset management. If we have proper asset management in the organization, we want to see whether the controls are, and by controls, we mean cyber security controls like perimeter security, endpoint security, proper authentication, proper authorization, network segmentation—these are controls. We want to see whether the controls are managed properly. We also want to see whether configuration is properly managed because software, hardware, operating systems, etc., if

configured incorrectly, may not be secure even with the right set of tools and technologies. Configuration and change management—so, whenever there is a change, are we doing it in the right way so that it does not expose the organization to further risk? Vulnerability management—do you routinely check for vulnerabilities, and do you fix those vulnerabilities in time, etc.? Incident management—how do you respond to incidents when there are cyber security incidents? Do you manage them in a reasonable way and within a reasonable time?

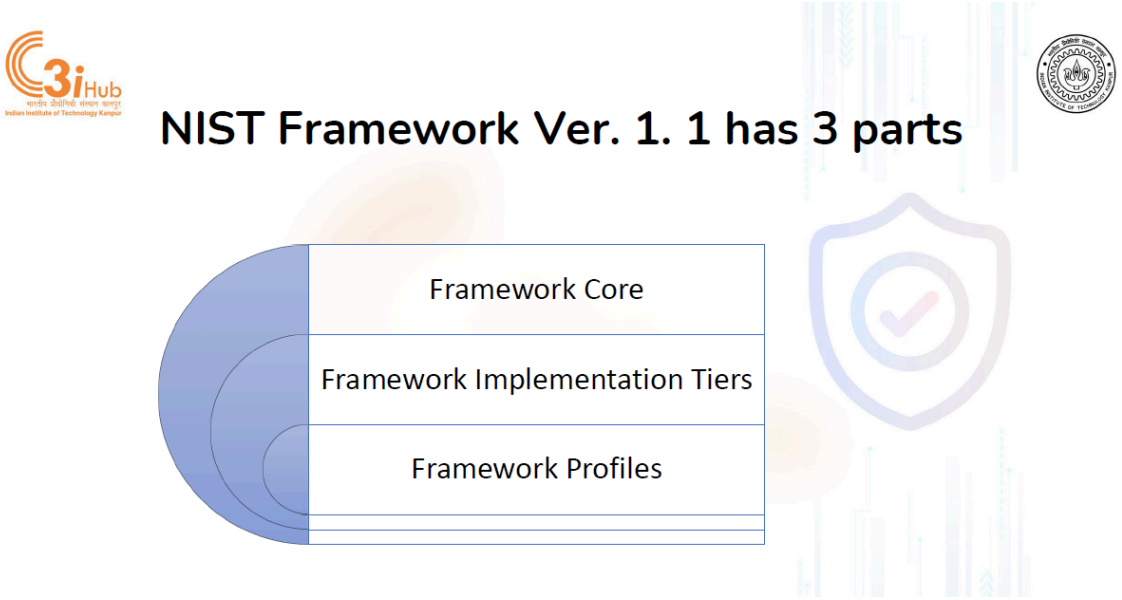
Service continuity management—how do you ensure that your services continue to be available to customers as well as internal users, even when there are cyber incidents? Risk management—do you conduct risk assessments and manage risks, etc.? Risk-driven cyber security. Now, external dependencies management—this is very important because external dependencies are basically third-party vendors, supply chains, contractors, and so on, who access your organization or provide products to it. You want to ensure that you check their cyber security because many attacks come through supply chains, contractors, or vendors having access to your network.

Whether you provide training and awareness—this is very important because, as we have said repeatedly, cyber security is about people, processes, and technology. The people part is very, very important. Even if you have the best security, but your users are not trained and they fall for social engineering, click on malicious links, and so on, your whole security might be rendered useless if a successful attack takes place when the user is socially engineered.

Now, of course, in a resilience system, even if the user gets socially engineered, it should not happen that the entire system collapses, but it can do some harm. So, we have to focus on training and awareness. Then, the situational awareness: this is where the security operation center, the security incident and event management tools, the network monitoring, the network, the endpoint monitoring—all these things come into situational awareness. We want to understand, on a real-time basis, what is happening inside my network, inside my endpoints, and accordingly how the users are behaving with respect to trying to, you know, log into things that they are not supposed to log into, whether they are trying to access a file system that is not supposed to be accessed by them, whether they are trying to get into a database that they are not supposed to be in, and things like that. So, this is situational awareness.

We will go into the details of each of these goals and the number of practices and the MILs. MILs are actually common across all these domains. So, we will go through the MILs once. Now, the way I have decided to do this is my slides will have a very abridged version of all these different goals and the related practice questions, but I will go into the

actual document to show you some of the goals and practices to give you an idea of how to think about them.



Now, in this context, as I already mentioned, the National Institute of Standards and Technology actually came up with this in 2018. They came up with the NIST Cybersecurity Framework or CSF. The initial version was 1.0, and then version 1.1 came up. Right now, as we speak, a few days ago—last week, I think—they released version 2.0, but we will not talk about version 2.0 because here we are discussing the resilience maturity model, which is based on risk, you know, CSF version 1.1.

Now, of course, the NIST framework is not an easy document to read unless you know a lot more about cybersecurity. But just to give you an idea about what the NIST Cybersecurity Framework is, it basically gives people a way of thinking in terms of how to organize cybersecurity in their organization, right? Otherwise, what may happen is that if you have not been trained in cybersecurity and you are an IT person, you are told—and this is happening in India also—that regulators often say to organizations that you have to have a CISO, right? Chief Information Security Officer. Now, if you are asked suddenly to find a CISO, there are not as many competent people in India, or not just in India—anywhere in the world—who are very well-trained CISOs in every organization. Of course, banks and all pay a lot of money to the CISOs. So, the best CISOs will now go to banks and maybe stock exchanges or stock brokerage firms and all that stuff. But if you think in terms of CISOs required in various manufacturing organizations, or especially smaller or medium-scale organizations or ports, for example, or things like that, you wouldn't get that many well-trained CISOs.

Now, this is a problem in the U.S. as well. The CSF activity started in 2013 with a presidential executive order by President Obama, which came as a fallout of the Stuxnet worm. Stuxnet was the worm that was used to harm the nuclear enrichment facility in Iran. They realized that critical infrastructure security was going to become very important in the coming years, and it has. So, they said, "Okay, fine. How do critical infrastructure companies, especially in the U.S., wrap their heads around what to do in terms of cybersecurity?" There are more than 1000 power companies in the U.S. that are very small and supply power to just one municipal region, or things like that. So, the question is, how do they wrap their heads around cybersecurity?

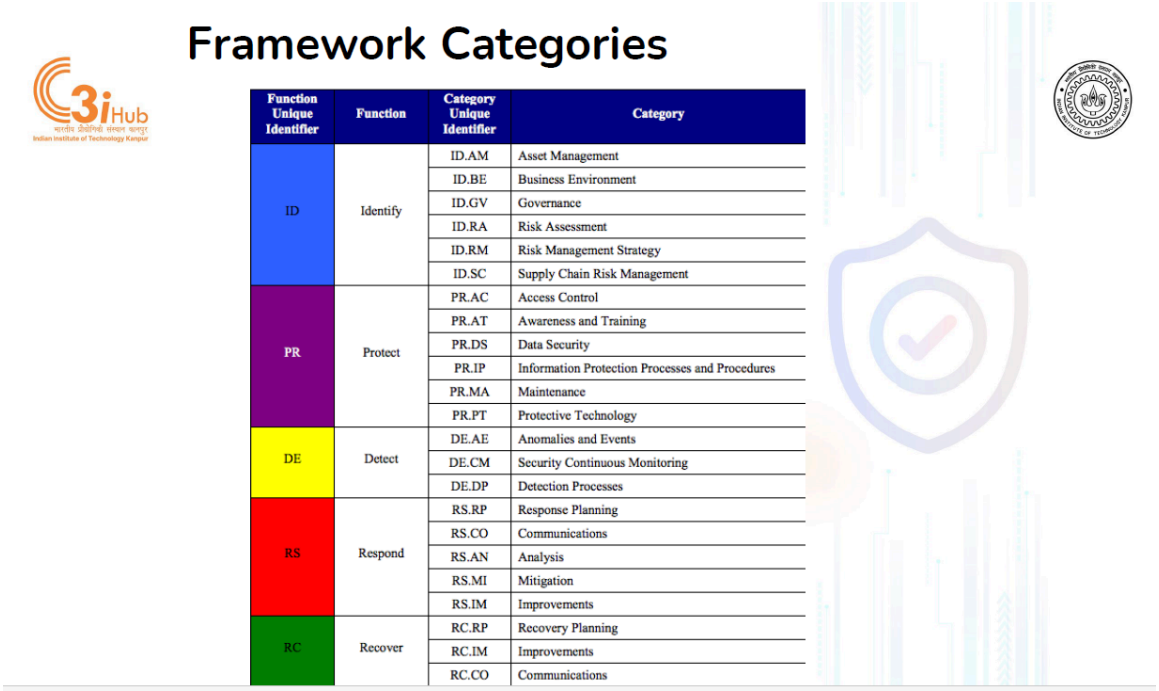
So, what the NIST framework came up with was saying that the first thing you have to do is implement five different functions. These functions are called identify, protect, detect, respond, and recover, right? Then, they said, "Okay, but not every organization is equally risk-prone." If it's a small mom-and-pop shop compared to, you know, a Walmart, they have very different risk profiles. So, you have to have different implementation tiers. You don't necessarily have to have the same level of sophistication in the implementation of all these five functions. That's why the implementation tiers were created.

Then, they introduced the notion of profiles. Profiles distinguish one sector from another. For example, you can have a profile for the banking sector, another for the oil and gas sector, and another for the maritime sector, ports, and other things. The reason these profiles are different is that cybersecurity in the BFSI sector is quite different from a power generation facility or power transmission facility. So, you create these profiles based on the sector you serve.

We will not go too much into the profiles, but we will talk a little about the functions. Now, in NIST CSF 2.0, there are six functions, and there is something called governance—cybersecurity governance. But let’s stick to version 1.1. Governance was part of "identify" in version 1.1. So, in "identify," you have to do things like asset management, identifying what cyber assets you have in your organization, including network devices, applications, firmware, hardware—everything—and figuring out what patch version they have, what kinds of vulnerabilities they have, etc. This is very important.

In asset management, you have to identify assets, and you have to identify the business environment, which has to do with risk assessment. The kind of business you are in and the services you provide will determine your risk profile and the kinds of threats you face. Governance was part of "identify," so governance involves having a CISO, a team under the CISO, and defining who is responsible for what kind of activity in terms of security. It also includes having a cybersecurity policy for the organization that is

implemented and enforced so that people actually have to abide by the policy. If the policy is violated, there would be penalties. This is part of governance.



Framework Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Risk assessment, as you have seen before, is very important. If you do risk assessment, you have to manage the risk. You have to do whatever is required to manage the identified risks. Then, there is also supply chain risk management, which is third-party risk management. These are the things you have to implement in "identify." So, even to implement "identify," you see that you have to do a lot of work, and it requires a lot of different skills, employees, tools, and technology. Once you have done this, now you have to think in terms of protection. The first line of protection is access control. You don't want a random person to log into your system or get into your system.

So, access control is very important. Initially, you would want to do this with authentication and authorization. Then, you want to make sure that even if you have logged into your system, it does not mean that you have access to every resource. You may have different segments of the network so that you do not necessarily have access to every resource inside your organization. Of course, awareness and training are an important part of protection because if your users are not aware of various threat models, what can happen through social engineering, what not to access, what not to do, etc., then you might have a problem. So, this is part of the protection.

Data security is about encrypting the data at rest, encrypting data in motion, all that stuff. Information protection processes and procedures—this is where the various processes and procedures that are followed for information protection come in. This might include

things like, for example, if you print out an important document, you have to shred it instead of throwing it in the garbage can. That will also be part of implementing this. So, cybersecurity is not necessarily always about technology. It might actually be something like a process or procedure. If you are found to have thrown away a document that is critical or marked confidential in the garbage can, then you will be violating a process or procedure.

Maintenance is important because, without maintenance, your systems will become old and unpatched, and then they will have attack surfaces. Then there are other protective technologies, which may include firewalls, antivirus, network intrusion detection, and so on. Protective technology is only a part of protection. We often think, "Okay, I have a firewall, I have antivirus, so I am protected." But protective technology is only a minuscule part of the entire protection function. You can see the importance of all these other things.

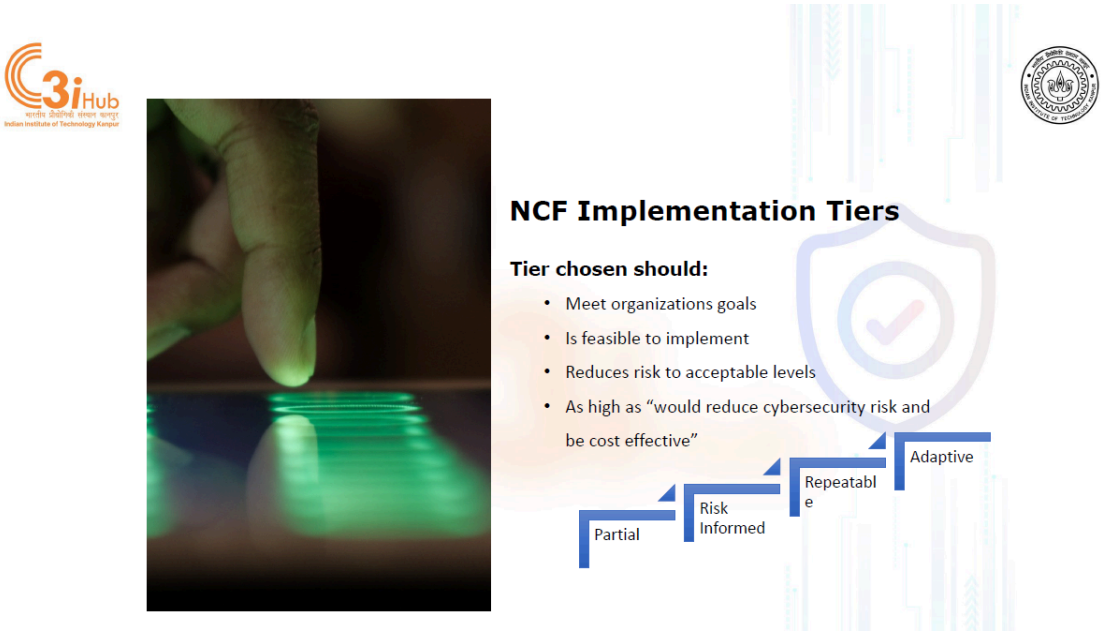
Now, the next thing is that, as we always say, attacks will happen irrespective of whether you provide the best protection possible. Therefore, you have to detect—you always have to be ready to detect through continuous monitoring of your organization, which is what we call situational awareness. So, you have to look for anomalies and events in the network packet stream, anomalies and events in the endpoints, that is, in the servers, applications, and so on, and you can probably get them from the logs. So, you have to do log analysis. This is continuous monitoring.

You cannot just do log analysis at the end of the day or the next day; you have to do continuous monitoring. There are detection processes that you have to properly put in place and define. Now, given that you are going to detect, sometimes you will detect an incident, and many times you will have incidents. So, you have to have a response functionality implemented, which includes pre-planning how to respond to each type of incident. There is usually an incident response playbook.

There is usually a very elaborate document called a playbook, and it might have, for every type of scenario or incident, what needs to be done, when it needs to be escalated, whom to inform, etc. This requires communication. We discussed this communication part in crisis management. Communication becomes very important for regulatory reasons. You may have to inform someone within six hours. You may also have to inform your regulator, your stakeholders, or the community that is using your system and services. For example, Microsoft is currently dealing with a Russian hack, and you see that they have communicated that to the rest of the world. Then, you have to do forensic analysis of what happened or what is happening, and you have to see whether you can mitigate it right away. For example, you might disconnect certain compromised systems from the rest of the system.

Part of the response is that, okay, this time an incident happened, and maybe I couldn't mitigate it, but I should be able to improve for the next time. That is the improvement part of the response.

Recovery is similar. If your system is compromised and your services are down, or if the quality of services is reduced, then you have to recover from that as soon as possible. Recovery planning has to be done long before an incident happens. There should be a plan for recovery. The first time an incident happens, your recovery might not be very fast, but you should be able to improve later to see whether, next time, if this happens, you can recover faster. Then, communications related to recovery—how long it takes, while you are recovering, keeping every stakeholder informed, and so on. This gives you a very quick bird's-eye view of what the NIST framework 1.1 functions are. Remember, identify, protect, detect, respond, and recover are the five functions, and then it talks about the implementation tiers.



As I said, the implementation of these five functions may not be possible in every organization to the fullest extent. For example, in some organizations, it may be ad hoc. Maybe I have a firewall, I have single-factor authentication, and I have some systems in a different network, but the majority of the systems are in the same network. I may have a little bit of endpoint detection through antivirus, but I do not have a SIEM tool or a SOC.

I would call that "partial." The idea here is that the organization is waking up to the idea of cybersecurity and trying to do certain things, but they are not doing it in a risk-informed way. "Risk-informed" means that I have done a detailed risk assessment, and based on which assets are in the highest risk category, I will put the highest level of

security there. I will focus most of my activities on those risk areas, and in other areas, I can do less. "Partial," on the other hand, is not risk-informed. So, they might unnecessarily do things for parts of the system that are least risky because they are flying blind and don't know which assets are at the highest level of risk.

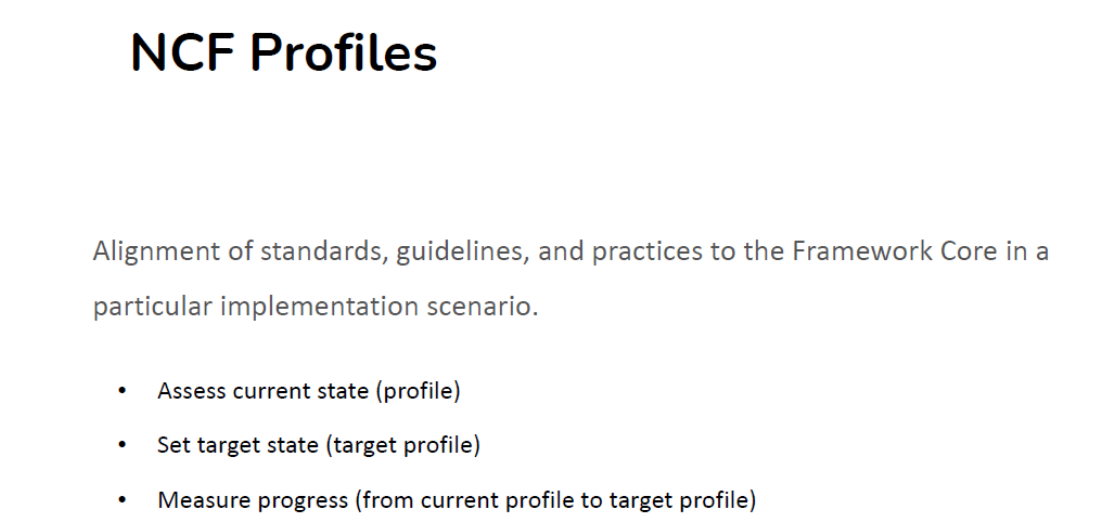
Risk-informed is better than partial. "Repeatable" is the next tier. Repeatable means that not only am I doing things in a risk-informed way, but I also have such good documentation, processes, and procedures in the organization that if the organization opens a similar facility elsewhere, I can just take whatever I have done in this facility and implement it there, and I will have good security. Repeatability requires very good documentation, processes, techniques, and so on. Everything has to be properly documented, reviewed, and kept up to date because the threat landscape changes, which means my processes and procedures will change over time. Repeatable requires that everything is not only documented and well-managed but also reviewed regularly so that the next time I go to a different facility and implement the same thing, I am using the latest technology and methods.

"Adaptive" is the highest level of maturity, where you are adaptive to organizational changes and to changes in the threat landscape. You can not only repeat your processes but also adapt to various unexpected changes. For example, if your company merges with another company, and that company's cybersecurity level is not as good as yours, an adaptive organization would bring the other part of the organization up to the right level of security, which would not happen if you are not adaptive.

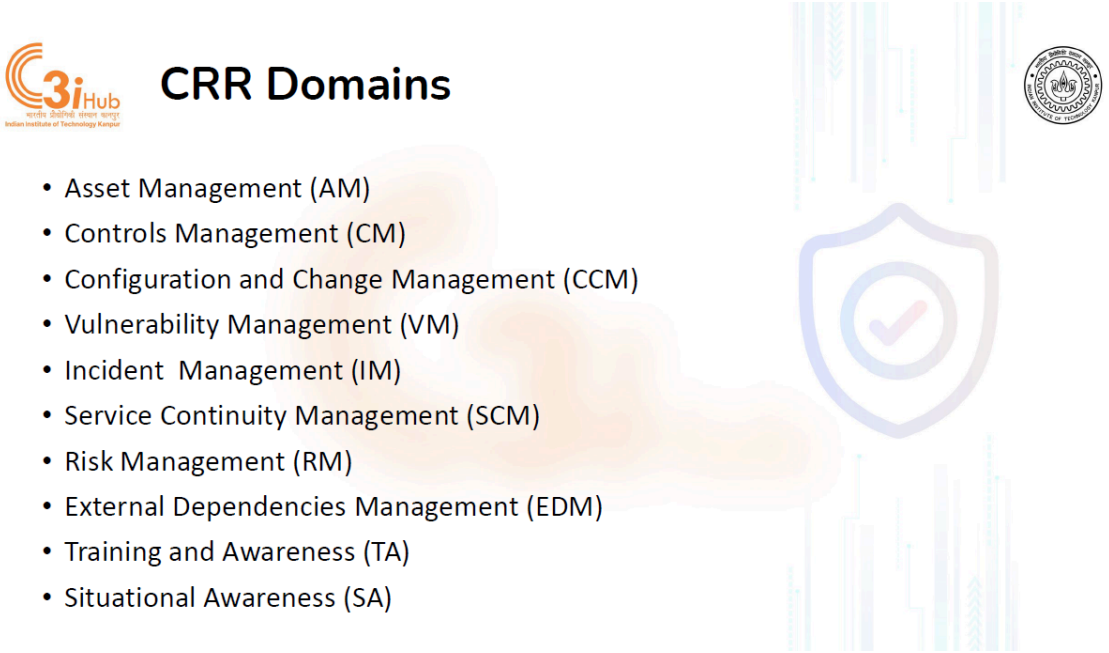
So, you have to then re-plan everything. So, these are the implementation tiers. So, we saw two things: one is the functions, five functions, or in the latest version, six functions, and then there are four tiers. Now, you have to see where you fit. If you are a small mom-and-pop shop, and you know you have a little bit of IT to scan the items and keep inventory, and a little bit of, you know, payments and everything online, you might be okay with partial for a while, right? Whereas, if you are a bigger organization, you may want to be risk-informed.

And then, if you have an organization with multiple different facilities, you want to be repeatable. And, if you are going to be a very large organization with a lot of dynamism, then you want to be adaptive. And, as I said, there are also NIST CSF profiles. Profiles basically talk about a particular implementation scenario. So, profiles will be different for the BFSI sector and the banking and financial sector, basically, and then it might be different in the power sector, it will be different in the maritime sector, and so on and so forth.

So, we will not worry too much about the profiles. So, now coming back to the domains, so we already saw what the domains are. So, we are going to actually, you know, use

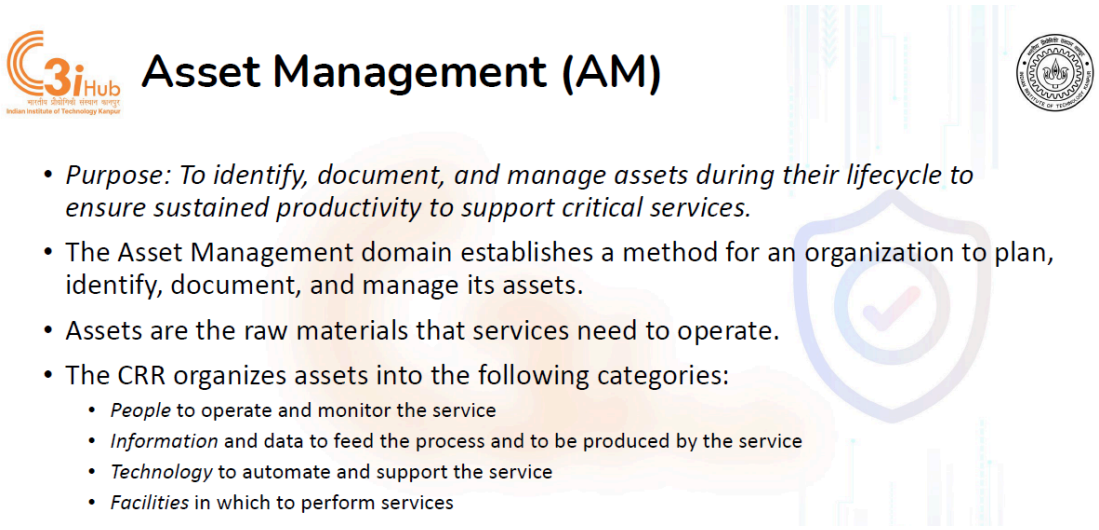


these abbreviations. So, for example, situational awareness I am calling SA, and asset management is AM, and service continuity management SCM, and so on and so forth.



So, now in the slides, I have these things kind of, you know, summarized and I will show you the actual document. So, asset management, so obviously every domain has a purpose. Asset management domain's purpose is to identify, document, and manage assets during the lifecycle to ensure sustained productivity to support critical services.

Now, you see that in this purpose, nowhere it says anything about security, right? The reason is that, see, security is at the service of security. Business continuity is at the



service of what the organization does. Security cannot be your main thing. So, when you do asset management, you want to actually make sure that when you commission the asset, like when you actually buy the asset, till the time we have retired the asset from the organization, it has to provide service such that you get productivity out of it for critical services, right? So, that makes sense, right? I mean, it does not have to be anything to do with cybersecurity except that the fact that this goal may be hampered by a cyber attack, right?

So, that is why I have to worry about cybersecurity. So, it is basically, this domain establishes a method for the organization to plan, identify, document, and manage its assets. So, you have to actually identify and document. So, you have to have a proper asset inventory, right? And then you have to manage the assets throughout its lifecycle. So, you have to know when it needs to be patched, when a vulnerability is reported, you have to know when it has to be upgraded, and so on and so forth.

Assets are the raw materials that services need to operate. So, assets are basically in the service of the business, right? Assets are not by themselves the most important thing. It is like, for example, this laptop is there for me to actually create the slides to teach you, not just, it is not like I need the laptop for the laptop itself, right? I need it for some activity. So, now we know that assets, we have seen this in the risk assessment module, that assets could be people, information, that is data, technology, and facilities. So, physical facilities, like a data center, for example, are an asset, right? So, you have these four types of assets: people, information, technology, and facilities.

So, it should be AM, asset management goals, here. So, asset management, ah. So, we looked at this earlier, we said there are seven goals of asset management. Now, you might say, why not eight goals or why not six goals? Now, this is something that after a lot of deliberations, people who came up with RMM came up with these seven goals.

7 AM Goals

- The Asset Management domain comprises seven goals and 30 practices:
  - Services are identified and prioritized (Identify)
  - Assets are inventoried, and the authority and responsibility for these assets is established. (Inventory)
  - The relationship between assets and the services they support is established. (Related)
  - The asset inventory is managed. (Managed Inventory)
  - Access to assets is managed. (Managed Access)
  - Information assets are categorized and managed to ensure the sustainment and protection of the critical service. (Categorized)
  - Facility assets supporting the critical service are prioritized and managed. (Priortized)

They hope, or they kind of convinced themselves that these are the different seven goals that kind of, you know, take care of all I want to, all I want to check in the asset management domain with respect to resilience, right? So, you might actually disagree, and you might want to split one of these into two goals because you think they actually have two different, you know, ideas. Or you might actually say that I want to add a new goal or things like that.

So, but as far as this one, the RMM is concerned. So, the first thing, we looked at this last time, services are identified and prioritized, right? So, I need to, I have all the services of the organization, whatever services it provides, have to be identified. And, whichever service is more important with respect to business continuity, with respect to the bottom line, needs to be prioritized. So, I need to know that these are the services I cannot let go down, and these are the services maybe for some time, if it goes down, I do not care, or I care, but not so much. Assets are inventoried and the authority and responsibility for these assets is established. So, every asset has to be part of a database called asset inventory.

So, there should not be any asset that is not known. And then, you have to know who is the owner of that asset, including, you know, applications. Usually, in a large organization, every application has an application owner and a custodian who has the responsibility, who is the custodian of the asset. So, that has to be properly documented in the asset inventory. It should not be the case that some asset is lying around, nobody knows whose it is and why it is there, and so on. Like it happened in a UP bank, like a couple of months ago, that some cyber criminals, they came in, connected a laptop to one of the open ports, DHCP ports, they got an IP address, and then they were in the network. And then they hacked into the core banking and siphoned off money. And for days and

weeks, nobody noticed that there is a laptop connected to one of the DHCP ports in the main, you know, front of the bank. And the attackers basically connected, got the DHCP address, and then went and remotely accessed with RDP to the bank, right?

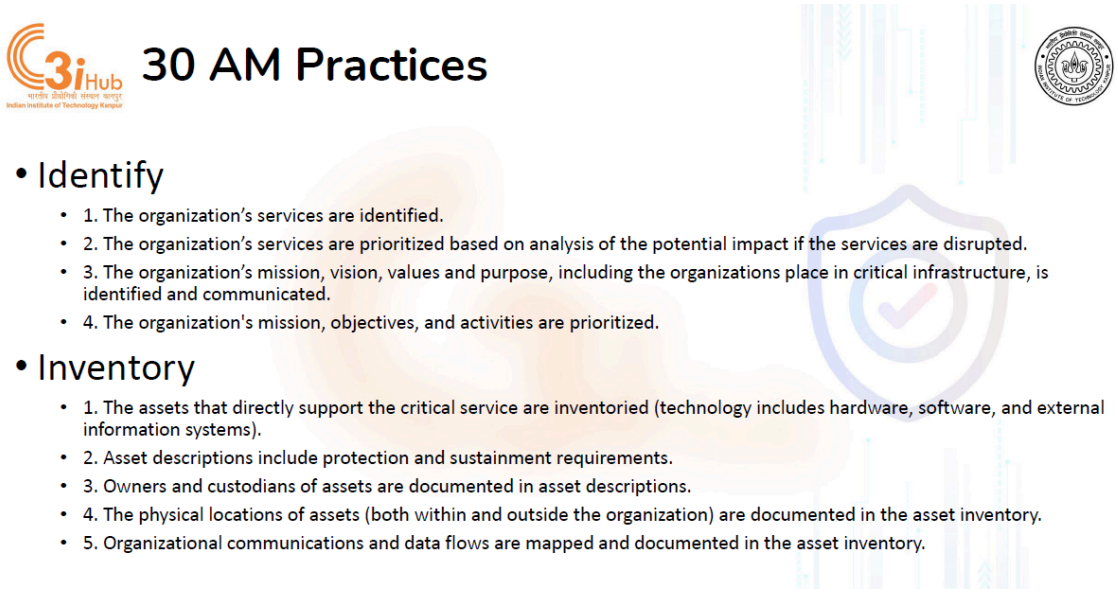
So, here you have an asset which is connected to your network. You have no idea where it is, right? That means there is no monitoring of the assets. Now, the relationship between assets and the services they support is established. So, you should know which asset is involved in what service because that will help. Here, you are saying that I have prioritized my services. I know which service is most important, which service is less important. Now, if I know which asset is in which service, then I can also accordingly prioritize the assets, right? I can say this asset is at the service of the most important service, so it is an important asset. The asset inventory must be managed, that is, the asset inventory should not be like it is an Excel file. When regulators come for an audit and they ask you for the asset inventory, you give them an Excel file, but you do not update that Excel file regularly, you do not automate the patches and all that stuff from the asset inventory, then it is not good, right?

So, you want to have a managed asset inventory. Now, also, access to assets is managed, right? So, depending on the priority of the asset, some assets may be accessible only by very high-privilege users, and some may be accessible to anybody. So, you have to decide, you know, which asset should be accessible by whom and accordingly manage the access. The information assets, that is, data, are categorized and managed to ensure the sustainment and protection of critical service.

So, the information assets are data, basically. Certain data is very important for operation, certain data is important because it is customer personally identifiable data. In any case, you have to categorize the data and then manage it to make sure that data is available and protected. Facility assets supporting the critical service are prioritized and managed. So, here we are talking about cyber assets, including software, hardware, firmware, etc., network assets, and so on. Here we are talking about data assets, right? And here we are talking about facility assets, such as data centers. For example, if a data center has an important critical service running in it, then that has to be properly prioritized and managed compared to, for example, a data center or server room that is not running important services for the organization.

So, now, there are seven goals, which are seven goals, and then, in these seven goals, there are questions that need to be answered, which we call practices. So, for example, to identify services, this goal will be checked against these four practices. These practices are like: organization services are identified, services are prioritized based on analysis of potential impact if services are disrupted, the organization's mission, vision, values, and

purpose, including the organization's place in critical infrastructure, are identified and communicated, and the mission objectives and activities are prioritized.

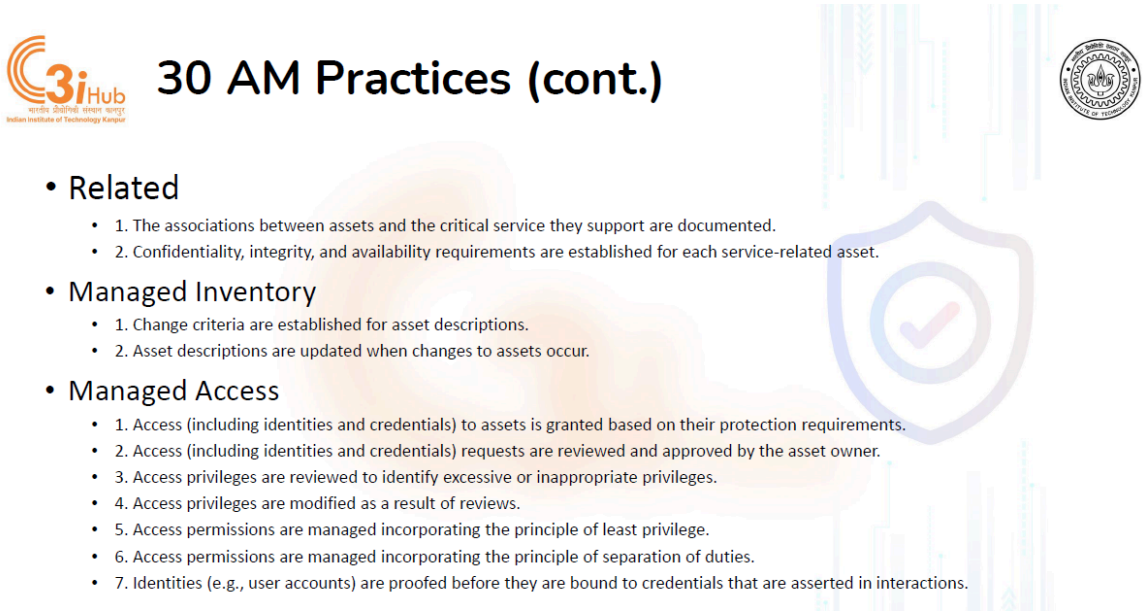


So, this is what we discussed last time from the actual document. So, if the answer to all of this is "yes," then we will say that this goal is met. If some of them are "no," then this goal has not been met. If some of them are "yes" and some of them are incomplete, that is, we do some of it but not fully, then also this goal is not met. So, this particular maturity model is also a winner-takes-all model. So, unless all four are "yes," we say that this goal is not met. If all of them are incomplete, then we say this goal is incomplete. So, that is one of the problems with this model. I have noticed that sometimes some of these might be incomplete, and still, you may have pretty good maturity, but this model will not give you good maturity; it will give you incomplete.

Similarly, if we go through this inventory thing, you say assets that directly support critical service are inventoried, right? So, it is basically saying, remember, the goal was that assets are inventoried and custodians and ownership have been established for every asset, right? So, here we are basically saying that assets that directly support critical service are inventoried, asset descriptions, including protection and sustainment requirements (like how you protect this asset and how you sustain this asset), owners and custodians are documented, physical location of the assets is documented, and organizational communications and data flows are mapped and documented in the asset inventory (like how the data flow happens). This is very important in terms of risk assessment and so on.

So, because some assets may be dependent on other assets and so on, this is the inventory practices. Then you have to say how the assets and services are related to each other. So,

the association between assets and services is documented, and confidentiality, integrity, and availability requirements are established for each service-related asset, right? For example, if you have a laptop for someone sitting at the reception, that asset may not require much confidentiality, maybe confidentiality, but not so much availability, for example, right? So, that kind of decision you have to document, right? Say which asset requires what security properties.



The next goal was that the inventory is managed. So, inventory is managed, that is, whenever there is a change in an asset or a new asset is included, that has to be put into the asset description, and asset descriptions are updated when changes occur. So, the inventory has to be managed; it cannot be left untouched after the initial creation of the asset inventory. It has to be continuously updated as per asset changes.

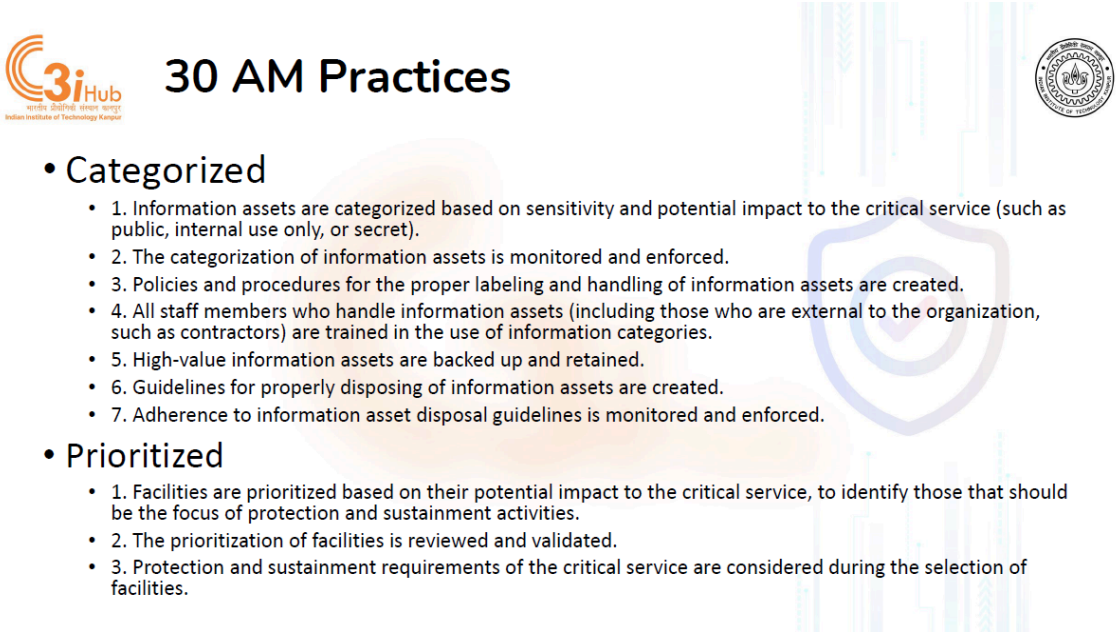
Managed access to the asset inventory, right? So, access to assets is granted based on the protection requirement. So, some assets, maybe a server that is part of your most critical service, can only be accessed by a privileged user, right? And then, access requests are reviewed and approved by the asset owner, right? So, if I am in charge of this particular server, I should be able to review who is given access. It should not be like, you know, some random other person gives them an account on that server.

So, you can have high privilege access or low privilege access. So, privileges are reviewed to identify whether there are excessive or inappropriate privileges. Like, for example, in IIT, most people use their laptops and computers with administrative privileges, right? In a company, that will never happen, right? So, administrative privilege is only given to very few people in the organization, right? So, if you need to install

software, you have to ask the system administrators; you cannot just willy-nilly install some software.

Now, what is good about that is that a malware you have downloaded from being socially engineered cannot run in a privileged mode, cannot run in administrative mode, and that way reduces harm. But, on the other hand, it is also annoying because, in order to install software, you have to ask the system administrator, who will actually then have to determine the risk, document it, and sign off on that risk before they actually install that software on your system. So, access permissions are managed, incorporating the principle of least privilege; that is, whichever person really needs this asset will only be given that privileged access.

Access permissions are managed, incorporating the principle of separation of duties. So, different people have different roles in the organization, and then you have to take that into account to see whether you need to give privileged access or access at all. And identities are proofed before they are bound to credentials. This is where you might do Aadhaar-based proof or give some kind of proof to actually know that this is really the person to whom you are giving access. Now, the other goals—I want to quickly mention a few things because it can take forever—so, categorized, right? So, the assets, you know, this is information asset data, right?

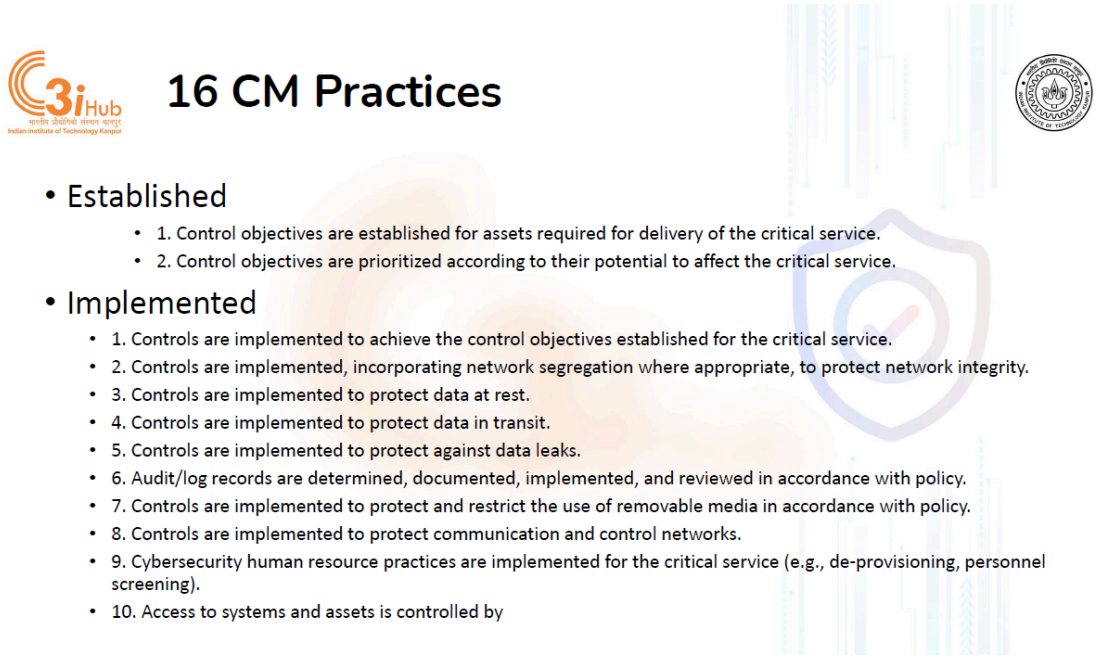


So, they have to be categorized. What is top secret, what is confidential, what is, you know, common knowledge, whatever, right? Then high-value information assets have to be backed up and retained. Guidelines for properly disposing of information assets: So, whenever you are done with a machine, you do not just throw away or sell the hard disk

to a random person, right? You have to write zeros and ones many times on the hard disk. This scrubbing, vertical scrubbing—you have to do all that. So, asset disposal guidelines are to be monitored and enforced. This kind of stuff. So, this is all about data protection and how you protect the data. And here, this goal, if you remember, was about facility assets, right?

So, facility assets have to be prioritized. Which facility, which data center, which server room, which factory floor, in the case of manufacturing or power generation facilities, have to be properly protected with physical access protection, right? And which facilities are high priority, etc., has to be reviewed and validated. And protection and sustainment requirements are considered during the selection of the facility. Some facilities may not be related to your important business services; you may not worry about that. But, if something is hosting assets—some physical facility hosting assets that are very important for your critical services—then you want to protect it by lock and key, access control, and so on, and video cameras, etc.

So that you know it is not being accessed by some random person. So, that is basically what we saw in this one, right? So, this asset management has these 30 practices that must be done in order to be considered mature asset management in the organization. So, we will talk about control management tomorrow.



We may not go through all the 10 domains—you can easily read it once you actually get an idea about, you know, how to go about reading these goals and the practices—but it will give you an idea about, if you were to work in an organization and if you are asked to actually think in terms of what will make the organization resilient, you have to think

about these different domains, you have to think about these goals and practices. That is the whole idea of studying this—to understand resilience and what resilience is all about and what you need to do to be resilient with respect to this model.

Of course, there may be a different model of resilience in which some of these things will be different. But, as far as this model is concerned, this is what you need to know and worry about to think in terms of resilience. Okay, all right?