Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

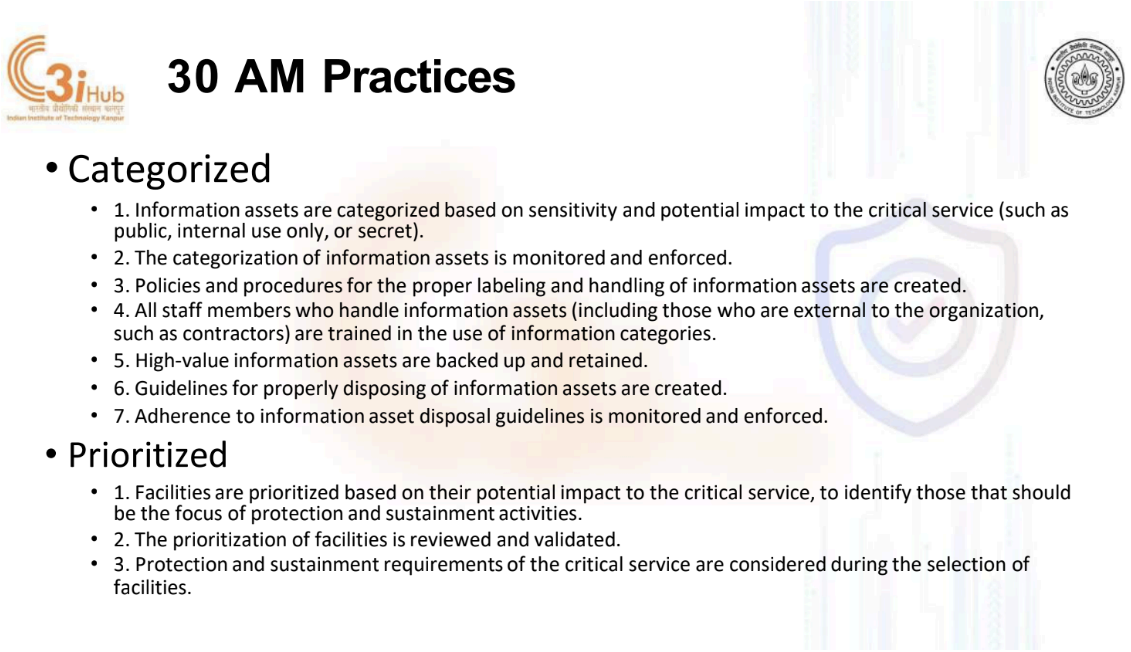
Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 24

Deep dive into Cyber Resilience-II

So I think it is time, so good morning everybody and so last time we talked about the asset management goals and asset management practices. And remember that for resilience what we need is the ability to recover as soon as possible when an incident happens and when an unprecedented or unplanned incident happens and you want to recover as quickly as possible. and without you knowing completely collapsing and keeping your service level agreements as intact as possible right. So, you should be able to provide some service, whatever the service that your organization is supposed to provide. Maybe with a reduced quality or reduced performance or reduced abilities, but at least you should not be completely collapsing and then when you recover you recover fast and the ability to recover to normal service level agreement is kind of a you know informal measure of what you know resilience is. So, resilience is more like elasticity right.



30 AM Practices

- Categorized
  - 1. Information assets are categorized based on sensitivity and potential impact to the critical service (such as public, internal use only, or secret).
  - 2. The categorization of information assets is monitored and enforced.
  - 3. Policies and procedures for the proper labeling and handling of information assets are created.
  - 4. All staff members who handle information assets (including those who are external to the organization, such as contractors) are trained in the use of information categories.
  - 5. High-value information assets are backed up and retained.
  - 6. Guidelines for properly disposing of information assets are created.
  - 7. Adherence to information asset disposal guidelines is monitored and enforced.
- Prioritized
  - 1. Facilities are prioritized based on their potential impact to the critical service, to identify those that should be the focus of protection and sustainment activities.
  - 2. The prioritization of facilities is reviewed and validated.
  - 3. Protection and sustainment requirements of the critical service are considered during the selection of facilities.

So, we discussed this before, and what we are saying is and maturity is basically to see whether a particular. So, for resilience we have to have certain goals the goal is related to whatever service you provide right. You may be an e-commerce business or you could be a power generation station or you could be a water pumping station or you could be a manufacturing factory or whatever you have certain services. You have to identify what your services are and then you have to figure out even when you have a cyber attack, can you actually provide those services? and if you are reducing the quality of service then how quickly you can get back to the normal services.

So, that is now to do that, I need to have goals and practices right. So, the goals are related to the services and practices are how to realize those goals or how to implement those goals. Now to do that you might be doing it in an ad hoc manner right. So, you might be doing like whatever is in the best to the best of your knowledge to the best effort you are trying to make sure that vulnerabilities are patched, the operating systems are updated, firmwares are updated, you are trying to figure out that your firewalls rules are as per norm you know as per threat intelligence that you have. You are trying to make sure that everybody has installed antivirus, you have ensured there is some network monitoring going on.

So, if there is some anomalous activity then some investigation is done. So, that is kind of ad hoc right and when you do this in an ad hoc manner the worst part of being ad hoc is that. you do not institutionalize the practices and processes. And so, whenever the lead lets us say the CISO leaves the organization things even again fall back to normal. You know, not non-challenged behavior, indifferent behavior towards cyber security. So, ad hoc is not good because ad hoc is often dependent on the personnel that are present during that time.

So, beyond ad hoc you want to do something that is more institutionalized which is the processes are accepted by the board or top level executives that these are the processes you must follow. And these processes there should be no exception to these processes like if you want to add an additional network router or you want switch you have to have certain testing done and you have to have certain you know put them in asset inventory make sure that it is passed on a regular basis its VAPT is done on a regular basis. So, you can set up a set of procedures for everything right. So, you can say if somebody wants to add a new application in the organization and if that application is going to run on a critical service server like the servers that are used in providing the important services then you have to have this kind of approval, this kind of testing and all the stuff. So, you can have something more what we call risk aware right.

I kind of analyze the risk. If I want to put in a new software I analyze the risk and if the risk analysis is done properly and I see that the risk is the benefit outweighs the risk then

I might do that right. Then you may want to do something more mature. For example, you may want to do like, you know not only you have the practices and procedures in place which are usually not accepted like you do not bypass the procedures, but you also review the procedures to see whether it is being effective or not right. because some processes are there often that there is a process because it is there in the books, but you do not actually have a benefit of it right.

If that is the case then you should revisit the process and procedures before you actually go further. So, that is where you do the reviews you have to do to review the process and assess the effectiveness of the process and practices. Compared to your goal, what is your goal right? And then finally, you know if you have all that stuff, then you have to also see whether you actually adapt to changing scenarios right. So, because threat landscape changes, business scenario changes, you might add additional business services functions.

So whether you can adapt to those things. So this is one way of thinking of maturity. So you start with an ad hoc like in the beginning of an organization doing thinking in terms of cyber resilience they might do it in ad hoc. It will kind of depend on the existing employees, their good wills and their interest and all that stuff. But from there you have to continuously strive to improve it towards an institutionalized process where it will become part of the organizational culture.

So, I will give you an example. We as IIT Kanpur or any government organization in India buys something like a laptop or a server or something. There is a process which is based on a very well written documentation called GFR right. So, the GFR, I think it is GFR 17 right now. It is a process by which a procurement happens.

A procurement requires, so, if I want to buy a server, let us say the server is supposed to cost about 5 lakhs, 6 lakhs, 4 lakhs, something I have and I have an idea. So, I have to first get a prior permission from higher authorities that this is the kind of money that needs to be spent and if that money is there. But once that is there we have to go through a process called tendering, right. In the tendering, we basically describe what is this thing that we want to buy, what should be its features and all that stuff and this has to be published for everybody to see. Then we may have a process for answering questions of prospective sellers prospective what we call bidders and then when we answer the question there would be a date for clarification deadline for clarification questions then we can answer questions.

Then after that we actually have to wait for the bid for the bid closing time and date. When the bid closes the bid cannot be in two parts usually. One part is the functional performance and other technical specifications of what they are offering and another is the price. They have to be submitted together but I as the procurer cannot look at the price information I have to first figure out among the bidders who satisfy my technical requirements which I put in my tender document. Once I qualify certain vendors, then another day another time I have to specify when I will open the commercial bids and then I will look at the price information.

and whoever has the least price, I will go for that. Now this is, there are certain variations of this in some type of procurements it may slightly vary, but I am just the for the exact process is not important in terms of what I want what I am going to say in terms of I am I want to make a case for what maturity what where the maturity not having maturity fails us. So, in terms of the process and procedure it is very institutionalized. No government institute in India funded by the central government or you know at least central government state governments may have a different rule I am not sure will not follow this process. So, the process, the practice is ingrained into the institution right.

So, that part is done. So, it is not ad hoc, it is not like I kind of decide that I will go to the Dell website and order a server, no I cannot do that. So, there cannot be anything ad hoc . It has to follow these practices. Also there are some committees to be formed. Like opening the bid and all has to be done in front of a committee and all that all that stuff.

But then the question is what is the goal of this practice right. The goal of the practice is to discover the price and rediscover the price that saves money for the government right. Eventually it is coming, it is taxpayers money. So, its government is holding taxpayers' money. So, the eventual goal is to save money to the extent that is possible. So, the price was discovered right.

So, the price discovery process is the goal. Now the question is that we have been following this since 2017 before that there was another GFR whatever. Now the question is have we ever done a review. Whether this is effective is whether we are actually getting the price that we should get right. So, that review process seems to be missing right.

So, nobody is reviewing, whether out of like you know 10000 I do not know like 100000 different procurements that happen in an institution, in how many cases we are actually getting the optimal price. And where if we are not getting it, where is the bottleneck, where we are, why we are not getting the optimal price right. This is the problem that you would see in many of the practices. There are good goals, the laws and rules are actually having good goals. but then eventually you will not get the maturity the process maturity is stuck at like between you know ad hoc and institutionalized.

So, I am not here to criticize a particular GFR or anything. It is a process that we all follow. But what I am trying to say is, maturity measures the effectiveness, assessing the effectiveness of a practice with respect to the goal that you declared. You have a certain goal right. The goals have been defined based on resilience in mind in this case and whether our practices are actually giving us the success with respect to the goals is very important for measuring the maturity of whether my practices are mature enough right. So, that is where all these things are coming from.

So, what you are what we are doing now like when we did the last time we did the asset management practices, we first said that there are 7 goals right that services should be identified and prioritized assets have to be inventoried and which asset is associated with which service needs to be mapped that is the this third one, the inventory has to be properly managed. It should not be like one time I put it in a spreadsheet and then I am done and in one month I buy another 500 different assets but I do not even put them there that cannot happen right. So, it has to be a fully functional inventory system. The access to this asset management system should be managed. Because otherwise and you know if you keep it open for anybody to modify then an attacker insider or outside attacker will come and modify your asset inventory right.

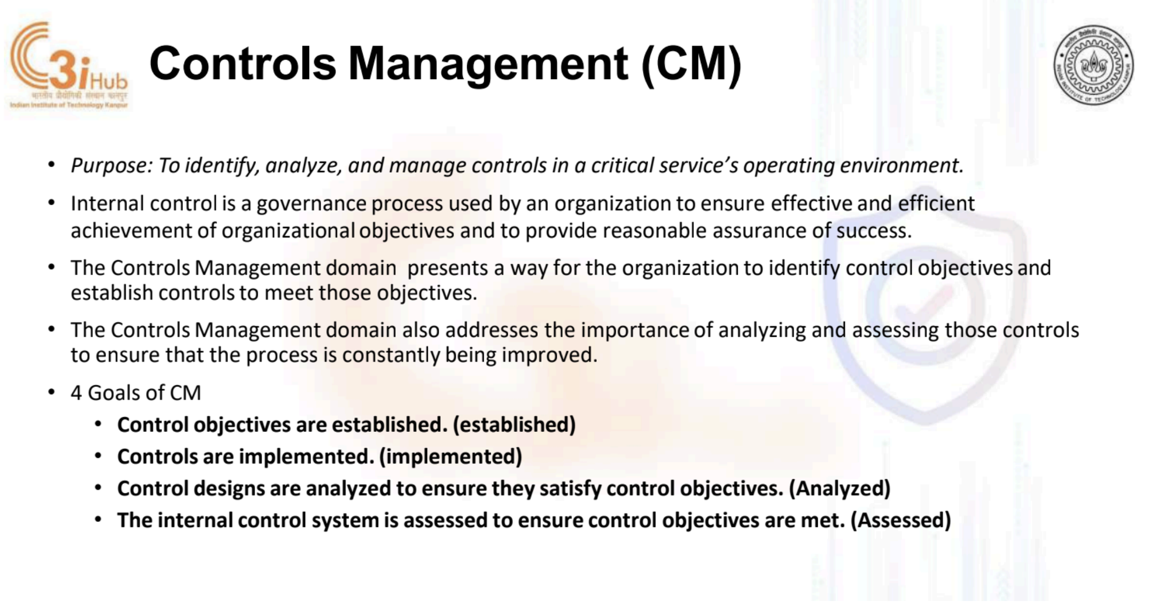
You will not even know that you have that asset. So, and then you have to categorize them based on how critical that a particular asset is. Not every server is in service of a very critical business function and then there are facility assets that also have to be protected like data center, server room, network room, network closets, all those things right. So, then we said that with respect to those goals. I have these practices.

So, now you might say that ok. So, to identify your assets. So, you are basically here for example, you are putting four different practices right. How would you, when you go to say an organization and want to check their resilience where they stand with respect to maturity of the resilience practices. You have to basically answer these questions: is this done, is this done, is this done and so on. Now in most cases, at least in this particular model by the Department of Homeland Security, we assume that the organization will answer these questions truthfully and honestly right, but they may not, right they might say yeah yeah we have all this right.

Now for the assessor, there is no way to know that they are lying or not. Like if they are missing half of their inventory or not how would I know as an assessor. I am going there for the first time, they might have like 15000 different machines and they are saying all of them are there all software, all application, all firmware everything has been inventoried I have to take their answer for it right. So, their answer could also be that you know it is incomplete. Now, I have to know how incomplete it is. It is just starting like they have put like first 100 out of 15,000 or they have put like 14,000 and then working towards 15,000.

So, there are a lot of gaps that are there in this model, right. This model is not a fool proof model for you know doing resilience assessment, maturity assessment, but at least you are somewhere. The reason why I actually wanted to go through is because see many times you are not even thinking that these are important things right. So, by looking at these practices you will know that these are very very important for an organization's cyber security. And you will also start appreciating the fact that cyber security is not just about procuring technology, like buying firewalls and buying intuition detection systems or access management systems and so on.

It has a lot more to it and that is why we say that cyber security is about people, process and technology. Technology is only one third of the entire cyber security activity. Now having said that, there are 10 domains this model decided that there are 10 domains across which along which I will measure the maturity right. Now why not 11 or why not 9. The answer to that and I do not. I have not spoken to these guys, but I have spoken to another maturity model coming out of the Pacific Northwest lab in the US.



Controls Management (CM)

- *Purpose: To identify, analyze, and manage controls in a critical service's operating environment.*
- Internal control is a governance process used by an organization to ensure effective and efficient achievement of organizational objectives and to provide reasonable assurance of success.
- The Controls Management domain presents a way for the organization to identify control objectives and establish controls to meet those objectives.
- The Controls Management domain also addresses the importance of analyzing and assessing those controls to ensure that the process is constantly being improved.
- 4 Goals of CM
  - **Control objectives are established. (established)**
  - **Controls are implemented. (implemented)**
  - **Control designs are analyzed to ensure they satisfy control objectives. (Analyzed)**
  - **The internal control system is assessed to ensure control objectives are met. (Assessed)**

They have a C2M2 model that is a capability maturity model for cyber security not for resilience, but for just for how good or bad their cyber security is. And in that model they also have 10 domains. So, the answer to the question is like why there are 10 domains. Because when we are also working on an Indian capability maturity model, cyber security capability maturity model for critical infrastructure. That is a project we are doing with the National Critical Information Infrastructure Protection Center.

This project is where we first came up with 19 domains. So, 19 domains like asset management is one domain, configuration management is one domain, patch management and change management is one domain, we have risk management one domain and so on and so forth right. So, we say we came up with 19 domains. And then we had a video call with the Pacific Northwest Lab and said, we are thinking 19 domains is like actually kind of adequate covering all aspects, how come you have only 10 domains and in their case they actually combine a couple of domains. Like for example, vulnerability management and patch management are combined in one domain, change and configuration management is combined in one domain right.

So, we ask them like why do you mix the two like of course, they are they have some relation, but why do you mix the two? So you say our sponsor said that there are 10 fingers on our two hands. There should not be more than 10 domains, right? Too many domains will make it difficult. And that is sort of true.

So to think in terms of a model. for measuring the maturity of cybersecurity or maturity of resilience, too many domains may actually make you very you do not even remember what are the 19 domains right. So, in our latest version of our model, which we started to pilot in many different organizations last month. We have 14 domains right. So, but I will leave it at that. I will not talk about our model. Maybe in the next version of the class I will talk about our model.

But here we have 9 more we just went through in detail on asset management in the last class. So, here is control management right. So, I will go through a couple of these models and it will be your job to actually go through all of them. And I will have some questions for you for the homework.

So, you can actually get some ideas. and of course, if needed we will discuss some of this in more detail. But if I want to go through each of them in very much detail, then the rest of the semester will be over and I will not be able to cover other topics. So, let us see what is control management, what is control? Whenever, whenever you have an organization running digitally, where various services with network and applications and an operating system and so on of course, you are exposed to cyber risks, right and we talked about risk assessment. When you assess risk you will see certain assets are at higher risk than at certain other assets. Certain assets are more critical for the organization than the other assets.

And accordingly you have to do protection of those assets which are higher criticality and then those which are lesser criticality there also you have to do certain risk mitigation. To do risk mitigation we do control right. So, control can be of two types right. So, one is technological control. That is you have a firewall, that is a technology control.

using firewall rules you block traffic that you do not want right. Similarly, you have controls like end point detection or antivirus which is controlling the possibility of an infestation of a malware into your systems. You have authentication and access control rights. So, you have two factor authentication or single factor authentication whatever. That is your defense against somebody trying to access your system.

or authenticated himself or herself into your system for you know by stolen identity and so on. You have controls like you observe the traffic. So, you have network intrusion detection. So, these are technological controls. So, normally when we write this, the RBI, Reserve Bank of India wrote a document called cyber security guidelines for all banks and banking sector companies back in 2016 and when they did that they actually wrote down many controls they said you have to have a firewall you have to have.

two factor authentication, you have to have antivirus, you have to have software you know has to be reviewed you know code code review has to be a practice for applications that you develop. So, they gave a list of controls, but there are controls which are not technological controls. There are more of what we call administrative control or process level control like for example, code review has to be done. This is not a technological control. You might use some tools like what we call SAST tools or DAST tools with static analysis or dynamic analysis tools on the software code to check whether it has vulnerabilities, but code review there is no better way than actually doing manual code review right ok. Manual code review can reveal a lot about, not only on you know flaws like buffer overflow or integer overflow or pointer null pointer access this kind of stuff they can also give you architectural problems with the code right.

So, code review that the fact that you have to do code review, whenever before you actually make a code live or the fact that you have to test the code in a test environment before and fast the do a fast testing or in an web application you have to check for top 10 OWASP web application vulnerability these kind of things are process control. Like these are controls that are not technology control, but control that are to be exerted by means of a practice and process right. So, now the question is that if I want to know whether our control management is mature enough, what should I check? What should be my goals? Now you see that here they are saying that four goals. First is control objectives are to be established right.

They are not saying what controls right. So, this is where I think RBI, SEBI etc., have made a thing. Although at the time they RBI and SEBI came up with their circulars it was very early. No other country or maybe very few countries in the world have their central bank come up with circulars on how to do security of the banks or how to do security of the exchanges and all other stuff. So, in that sense they did pretty early which helped the banks and all to know what exactly had to be done before even they were very aware of cyber security.

But in general what we say is that you should not tell them what controls they should exert. They should know their risks and based on the risk they should design their control. So what we need to check is whether based on risk ratings they have figured out which controls need to be there right. So the maturity is not in which controls they have, but maturity is in self figuring out what controls will reduce their risk to below their acceptable risk, right. Then the next thing is we have to check whether controls are implemented.

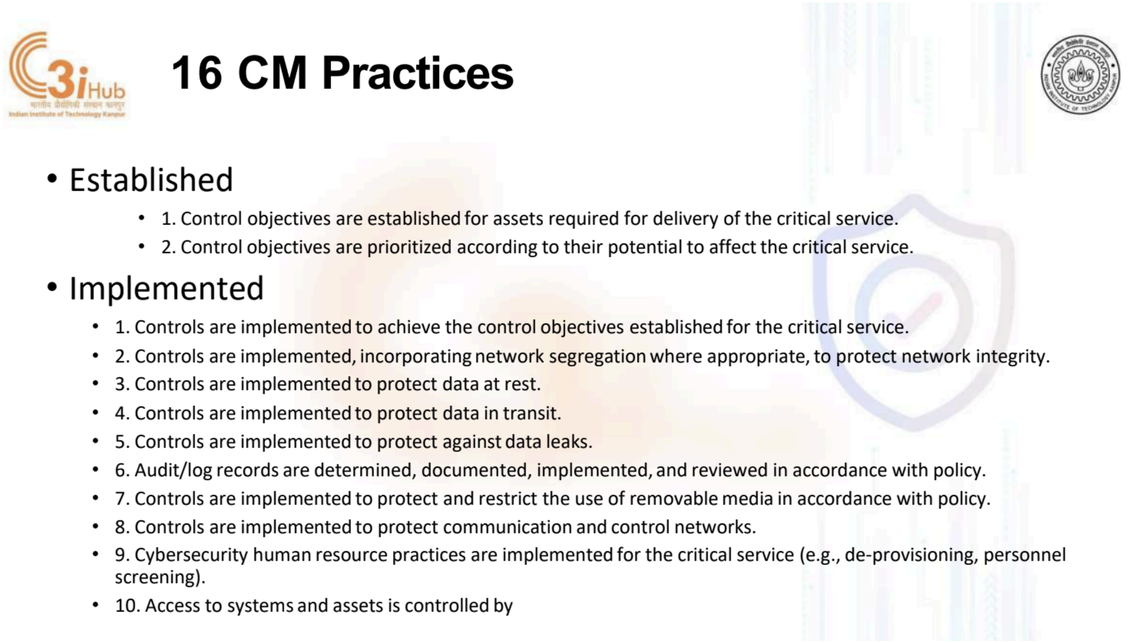
Now how do you check whether controls are implemented? This has to be checked against the previous one. Remember the previous one. says the controls are established. How do I check the controls are established? I read their policy document.

Every organization should have a cyber security policy document. That document should say what controls are there and these controls are not necessarily all about technology. For example, it might say that in the organization people are not allowed to connect their own phone into the network of the organization right. Or they are not, if your laptop has two network interfaces, you cannot connect the other interface using your data. and one connects to the other interface connected to the network of the organization. This may be disallowed depending on the risk profile of the threat profile of the organization.

But so what I am trying to say is the policy document does not say that ok does not only say that you have to have firewall, you have to have individual windows firewall up, you have to have you know you cannot turn off your antivirus in Windows Defender in your in your machine and so. These are technology control but you can also give control on behavior like for example you can say that you are not allowed to go to social media from your work network, right. You may, I mean depending on the organization's own risk perception right does not have to be that that that control. So, control objectives are written in the policy document and then the auditors will come in and ask you for the policy document and say ok let me see your policy. First thing they will check is the policy document is meaningful comprehensive etcetera etcetera based on their risk profile right.

Then, they will say ok let me see if you have actually implemented these controls or you are just writing that these controls are there, but nobody bothers about it right that is quite possible right. So, there may be a very nicely written control of the policy, but nobody is doing anything about it right. So, that is what the auditor's job is to check against this policy right. And, then control designs are analyzed to ensure they satisfy control objectives.

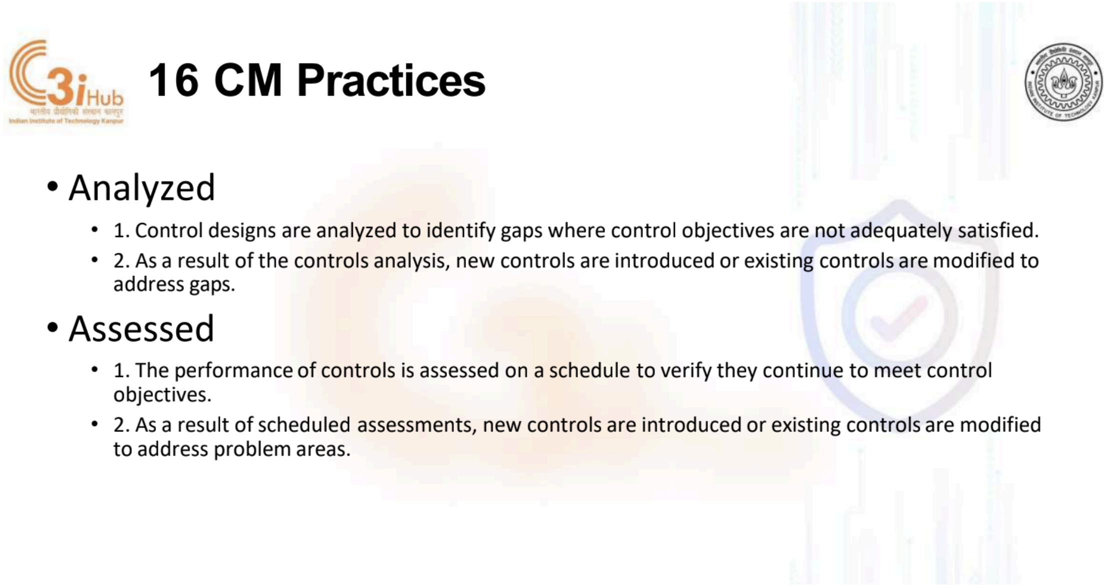
So, this is where I was talking about maturity right. So, when I have a tendering process, I routinely analyze the tendering process to see whether it is actually meeting the objectives for which this tender, this rigorous tendering process was invented. So, control designs are analyzed to ensure that they satisfy the control objectives and this is where the control objectives are established. And then you have to see whether the internal control system is assessed to ensure control objectives are met right. So, here you are analyzing that the objectives are being met and here you are assessing whether your control objectives are being met.



16 CM Practices

- Established
  - 1. Control objectives are established for assets required for delivery of the critical service.
  - 2. Control objectives are prioritized according to their potential to affect the critical service.
- Implemented
  - 1. Controls are implemented to achieve the control objectives established for the critical service.
  - 2. Controls are implemented, incorporating network segregation where appropriate, to protect network integrity.
  - 3. Controls are implemented to protect data at rest.
  - 4. Controls are implemented to protect data in transit.
  - 5. Controls are implemented to protect against data leaks.
  - 6. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
  - 7. Controls are implemented to protect and restrict the use of removable media in accordance with policy.
  - 8. Controls are implemented to protect communication and control networks.
  - 9. Cybersecurity human resource practices are implemented for the critical service (e.g., de-provisioning, personnel screening).
  - 10. Access to systems and assets is controlled by

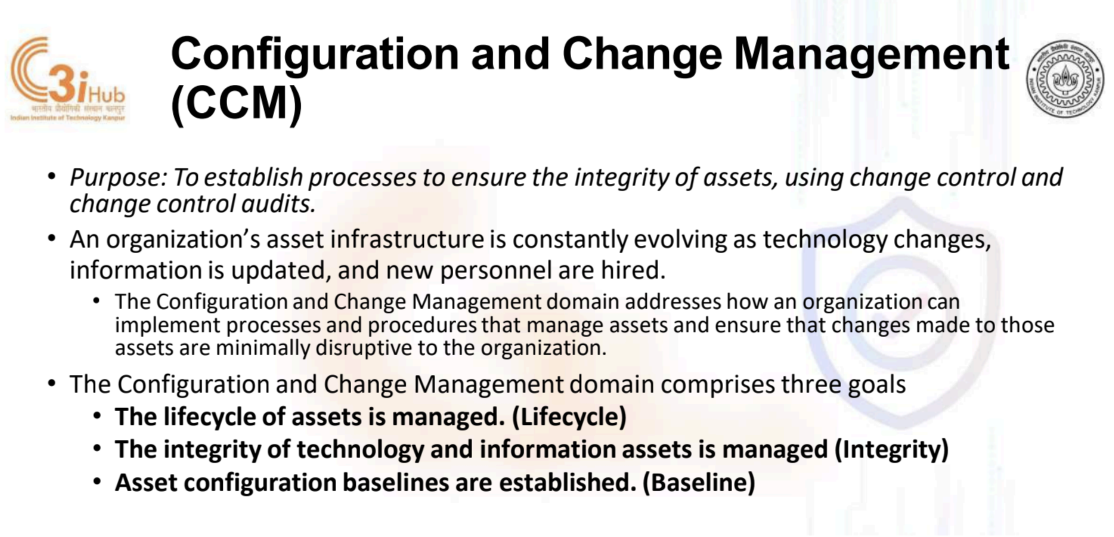
So, this is the meta level analysis. So, I am not going to go through the practices. So, to establish control so, you see that again for the assets that are required for delivery of critical services, we have to make sure that their control objectives are properly, you know established even if you do not do it for non-critical the assets that are involved in non-critical services and then you have to prioritize which one can affect the critical service. Now here you will see if you look at a cyber security maturity model versus a resilience maturity model. This difference in the cyber security maturity model will not say only worry about the critical services. We will say worry about all services right, but here we are saying only worry about critical services because remember in order to be resilient, you have to assume that attacks will happen.



16 CM Practices

- Analyzed
  - 1. Control designs are analyzed to identify gaps where control objectives are not adequately satisfied.
  - 2. As a result of the controls analysis, new controls are introduced or existing controls are modified to address gaps.
- Assessed
  - 1. The performance of controls is assessed on a schedule to verify they continue to meet control objectives.
  - 2. As a result of scheduled assessments, new controls are introduced or existing controls are modified to address problem areas.

It is only that the critical services should be still available even when the attack is ongoing or at least it should be available at a reduced scope or reduced quality. If not then the recovery has to be very fast. So, critical services are focused on in the case of resilience. So you can go through these different practices. I am going to let you know some questions for doing homework so you can get through this. Now configuration and change management right, so that is the next domain right, so this is the third domain.



Configuration and Change Management (CCM)

- *Purpose: To establish processes to ensure the integrity of assets, using change control and change control audits.*
- An organization's asset infrastructure is constantly evolving as technology changes, information is updated, and new personnel are hired.
  - The Configuration and Change Management domain addresses how an organization can implement processes and procedures that manage assets and ensure that changes made to those assets are minimally disruptive to the organization.
- The Configuration and Change Management domain comprises three goals
  - **The lifecycle of assets is managed. (Lifecycle)**
  - **The integrity of technology and information assets is managed (Integrity)**
  - **Asset configuration baselines are established. (Baseline)**

Now remember that every software you know about hardware operating systems has thousands of different configurations right, firewalls and network devices routers and so on. So the question is what is the configuration that you should choose to ensure that your probability of getting attacked is reduced right. So, that is very important and that is what is called configuration management right, you have to do the right configuration. For example, you can you can bring in a windows machine connect to the network, but you do not use windows firewall, you do not use windows defender or any antivirus, you do not put a password for screen lock, you do not you know do any kind of control on who can execute the PowerShell. You can make all kinds of mistakes in configuring a particular machine that you are connecting to the network right.

Then that machine can easily be a you know kind of a conduit for virulent attacks. So, now it is their responsibility to configure that machine right. Now you cannot leave it to individuals especially in an organization some individual might say that I want an administrative account on my windows machine right.

I want to be the root right. No company will allow that right. For some reason we allow that in IIT. But no company will allow that. If you are connected to my network, you cannot have administrative control because of administrative control. You can run powershell, you can configure SMB, you can downgrade the windows whatever you want to do and get my entire network into trouble. So, what I will do is I am going to configure your machine and take out your administration.

If you want something to be installed which requires administrative control, there should be a trouble ticket system or some kind of an online system by which you apply for that software to be installed. And then, the person who is in charge of installing all this making sure configuration is correct will come and install it for you or remotely install it for you depending on how the configuration is. This is what I have done back when I worked in industry in the 1990s . This was the case even though you know that time it was the time of Windows 98, right. So now, obviously this is what all organizations will practice. Nobody will give you full access to your work computer.

if you are given full access, then they will install something called an MDM. right device management software which will report everything you do to a centralized observation system. So if you are going to run PowerShell, if you are going to install a new software on your machine all that information will go to that central observer. And if they find that is anomalous, they will stop you or disconnect your computer from the network from their network right. It should be the right of the organization that if you are connecting to their network you are endangering their network and in turn all the other users of that network therefore your rights should be limited right what you can do and what you cannot do. Now you might say that if I am a developer, I need to compile new software and run new software.

If you whitelist all applications on my machine, I cannot do development. So, developers are usually in a segregated network. They are not, they are disconnected via firewall, not disconnected, but mediated through firewall their network from the rest of the operational network, so that in case. So, the developers' machines will have all the flexibility of administration, administrative control and so on, but then they cannot really be in the same network. If they have to access something from that network to the operational network they have to go through the firewall and go through access control mechanisms right. So, that way you can reduce the possibility of any harm that can come by having more flexible machines in their disposal.

Another thing that is very important is that, whenever we, so, whenever a machine is done with say I have a machine for 5 years a laptop or a desktop or a server and I am done with it I dispose of it. How do you dispose of it right? So, you know in many cases you will see that the dean will send an email saying that the so and so department is disposing of many machines if you want some of it collected right. Now most likely that we do not have much confidential information in those machines but in case there is a database of all students and their phone numbers and other numbers are there then there is a problem right. So there should be a proper way to dispose of the disk erasing software that will actually erase this thoroughly right.

This is why the confidential information has to be completely scrubbed from these machines. And as assets are removed from the service the asset inventory must reflect that properly right. The asset inventory should not be having stale information. So, the life cycle of assets has to be managed right. The integrity of the technology and information asset is managed by the integrity of the technology information asset. How many of you have heard of the XZ vulnerability that is affecting almost all Linux versions last week right?

So, XZ is a compression software like a tar right tar and zip gzip. It is apparently used very heavily on almost all Linux distributions including Ubuntu and Fedora and CentOS and everything right. Now it turns out that XZ is a free software right. It is an open source GitHub based software somebody posed as a developer and introduced backdoor into it and now it has gone into almost all Linux versions right. So, anybody who is running a Linux now if they have not upgraded their Linux do it right away because it is a severity 10, the highest most critical severity vulnerability that is sitting in your machine if you have not upgraded it. If you are an automatic upgrade by now you must be upgraded already if not then you should upgrade this.

Now this is whatever the integrity of the software is right. So this is a big problem right? So there is one very few people who even know that there is an XZ thing. the compression utility that is in the software bill of material of almost all Linux distributions and the fact that some if somebody does something there. and it gets nobody notices it in this github and then it gets integrated into all the latest updates of all this software then all this software becomes vulnerable right. So, this is something that requires knowing what every software that you are using needs to know what are the dependencies.

And nowadays like things like Linux, even Kali Linux is affected by XZ, right. So, if you know this you have to know what SBOM is what we call SBOM the software bill of materials for every software. All that all the dependencies, all the libraries and all the software dependencies must be very transparent to that organization. Hopefully it should also be you know not only transparent to the organization, but also it should be it should be automated that is Any time any CVE is declared for a particular software automatically your all your SBOM should be checked for every CVE to see whether that particular software has been affected and you know what needs to be done whether the patch is available. If not , until the patch is available you may have to do something like shut down or do some mitigating action right.

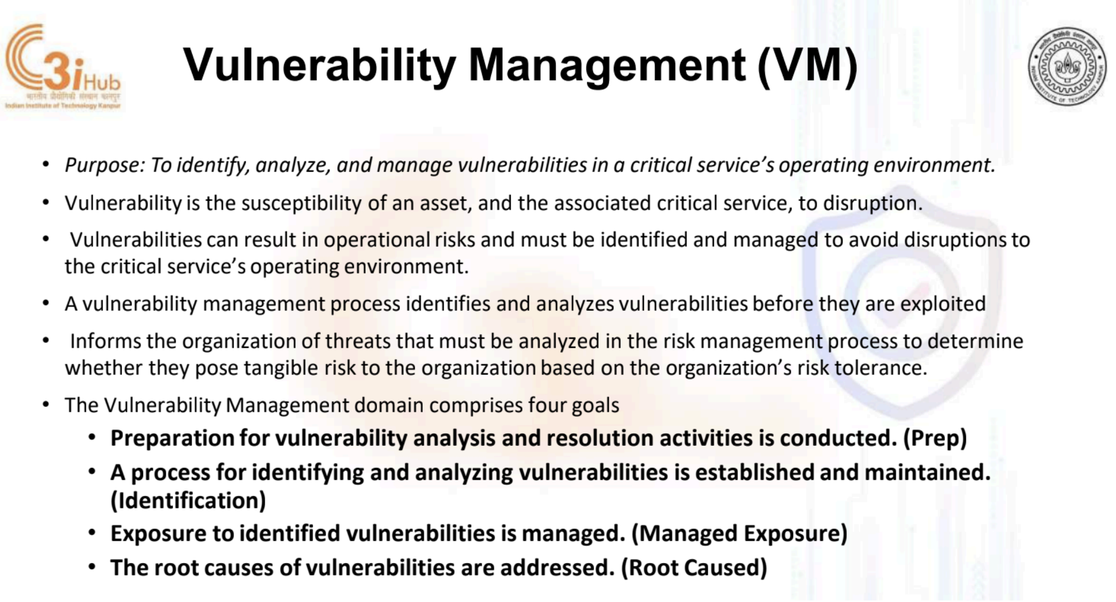
So this is the integrity of the technology and asset configuration baselines are established, right. So this baseline thing is done very well by the US Department of Defense, right. So the US Department of Defense has defined something called a STIG. security technology implementation guide right. So, actually the MITRE corporation and NIST came up with this suite of standards. And in this set of standards they actually defined language usually based originally in the XML, but then later on in JSON form by which you can have standard language for describing you know software hardware their versions and so on stand it is called CP common product enumeration.

then CCE common configuration enumeration. So, there is a language for describing configuration, there is language for describing vulnerability and so on. So, using this they have this benchmark files format formalized benchmark files. These benchmark files are in XML and this benchmark files tell you like. So, there is a benchmark file for all Firefox version XYZ, all chrome version XYZ. What does it do? There is software which you can run with this benchmark file and each benchmark file has multiple profiles.

For example in the benchmark file there would be parts which will apply to those systems which are critical. Then there are parts which are less stringent that are meant for not so critical systems and so on. So, you can use the scanner and this scanner will take the benchmark file and ask you within the benchmark file which profile confidential profile or critical profile some which profile you want to check against. It will automatically check your Chrome or your Firefox's configuration against that benchmark set of configuration.

So, this is called STIG benchmarking Security Technology Implementation Guide based benchmarking. So, when you do the STIG benchmarking, it will give you a report saying that look here your Firefox has this configuration problems with respect to my baseline benchmark right. So, initially the Department of Defense published and they still publish on the DoD website a huge amount of benchmarks like for Windows 11, for Windows 10, for various versions of Linux and so on, various applications, firewalls and so on. For everything they have a benchmark file, you can run a scanner with that benchmark file and see whether your configuration is secure with respect to that baseline benchmark. Not only that as an organization you can there are ways to edit that benchmark file.

So, you can edit the benchmark file to suit your organizational needs or new threats and so on. Now the question is that this baseline file also has an organization called CIS right. So, CIS now has a whole lot of STIG benchmarks right for various software hardware you know operating system applications and so on. You can also, it is not difficult to learn the language of STIG, so as an organization you can write your own STIG files. And we have been telling the organizations in India like CERT-IN to actually publish a STIG benchmark for government computers so that all the government departments can run this STIG benchmark against the baseline defined by CERT-IN and then check whether it is according to the benchmark. So, this establishing this benchmark is very important right because otherwise how would in the same organization two departments might have different baselines right and they somebody will leave a lot of things in insecure configuration and another department will make it secure, but since the other department is insecure that will affect this department.

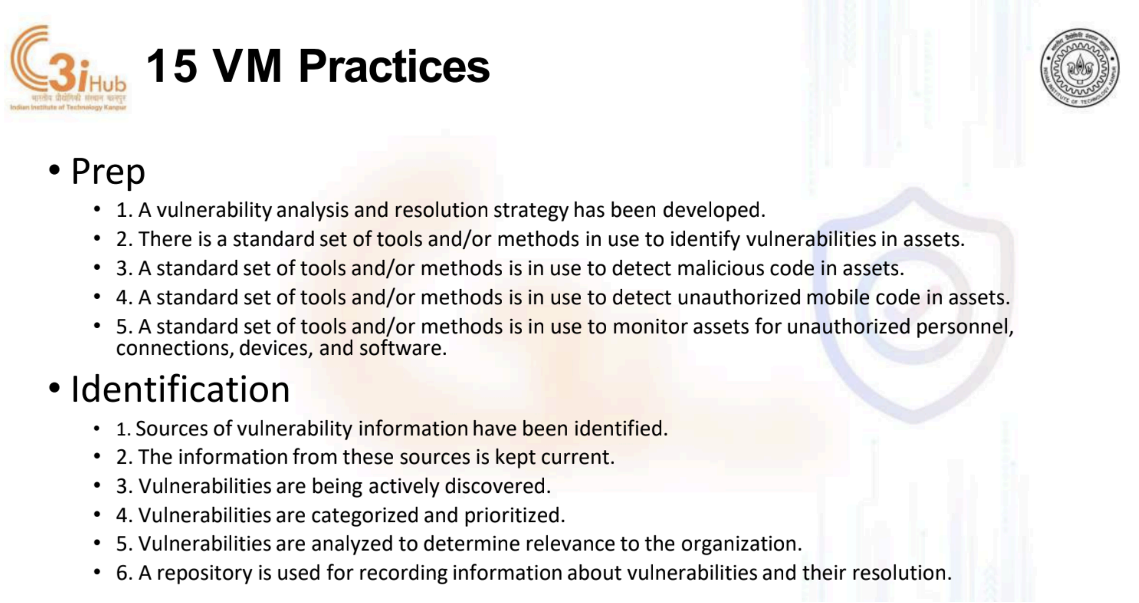


Vulnerability Management (VM)

- *Purpose: To identify, analyze, and manage vulnerabilities in a critical service's operating environment.*
- Vulnerability is the susceptibility of an asset, and the associated critical service, to disruption.
- Vulnerabilities can result in operational risks and must be identified and managed to avoid disruptions to the critical service's operating environment.
- A vulnerability management process identifies and analyzes vulnerabilities before they are exploited
- Informs the organization of threats that must be analyzed in the risk management process to determine whether they pose tangible risk to the organization based on the organization's risk tolerance.
- The Vulnerability Management domain comprises four goals
  - **Preparation for vulnerability analysis and resolution activities is conducted. (Prep)**
  - **A process for identifying and analyzing vulnerabilities is established and maintained. (Identification)**
  - **Exposure to identified vulnerabilities is managed. (Managed Exposure)**
  - **The root causes of vulnerabilities are addressed. (Root Caused)**

So, institute wise or organization wise the benchmark should be established. So that is what they want. So, you can look at these CCM practices. Vulnerability management is what are the goals? So, first of all you have to continuously know what vulnerabilities are there in your systems right. So, you have to prepare for vulnerability analysis and if you find a vulnerability you have to know how to resolve the vulnerability, resolution activities have to be conducted. The process of identifying and analyzing vulnerabilities is established and maintained.

You have to do an audit . There are vulnerability scanners like you can have the Nessus scanner right. So there are many such scanners you can use. Open source scanners are also there so you can scan for vulnerabilities. But none of the scanners will be able to discover everything because there are nowadays software whose dependencies are extremely deep right. So, for example, 2 years ago there was this log4j vulnerability that came up. The Log4j vulnerability is actually a very specific version of the Log4j library that was affected.



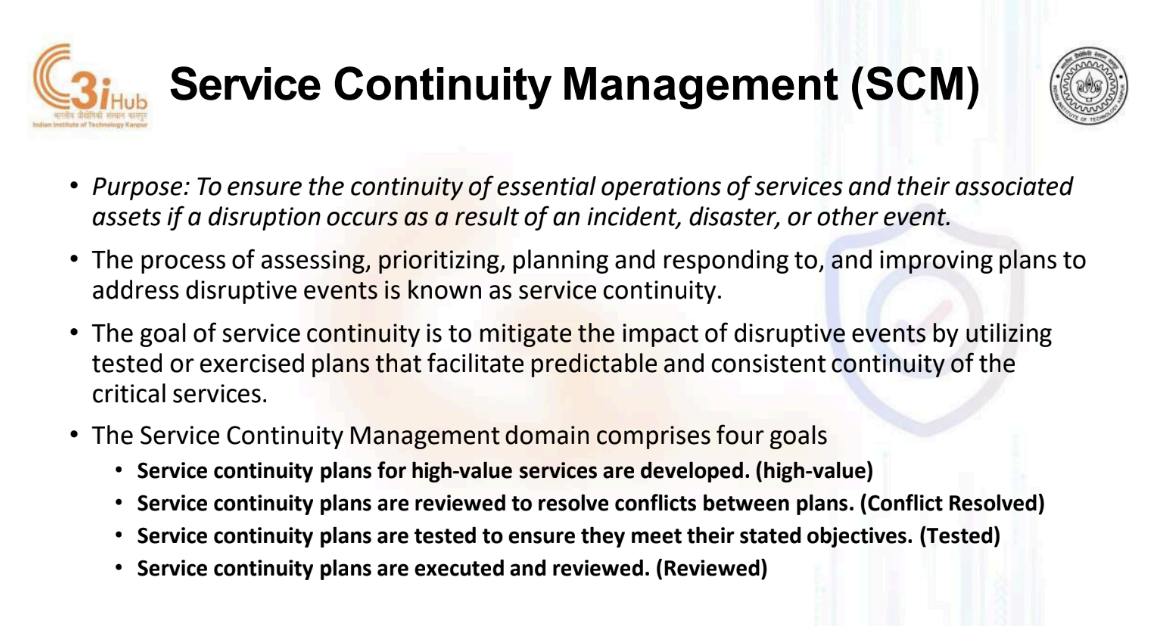
15 VM Practices

- Prep
  - 1. A vulnerability analysis and resolution strategy has been developed.
  - 2. There is a standard set of tools and/or methods in use to identify vulnerabilities in assets.
  - 3. A standard set of tools and/or methods is in use to detect malicious code in assets.
  - 4. A standard set of tools and/or methods is in use to detect unauthorized mobile code in assets.
  - 5. A standard set of tools and/or methods is in use to monitor assets for unauthorized personnel, connections, devices, and software.
- Identification
  - 1. Sources of vulnerability information have been identified.
  - 2. The information from these sources is kept current.
  - 3. Vulnerabilities are being actively discovered.
  - 4. Vulnerabilities are categorized and prioritized.
  - 5. Vulnerabilities are analyzed to determine relevance to the organization.
  - 6. A repository is used for recording information about vulnerabilities and their resolution.

But the vulnerability was extremely severe. At that time most organizations it turns out that almost all organizations around the world have some dependency on Log4j. right even if you do n't know that you are even using Java anywhere it log4j is a Java library but there are Java dependencies. So not scanners will give you some information but you have to have a more in-depth analysis of your software bill of materials and what software dependencies are there. And then exposure to identified vulnerability has to be managed right. So what does it mean? Now one thing is to fix the vulnerability by doing an update or upgrade of the operating system, upgrade of the version etc.

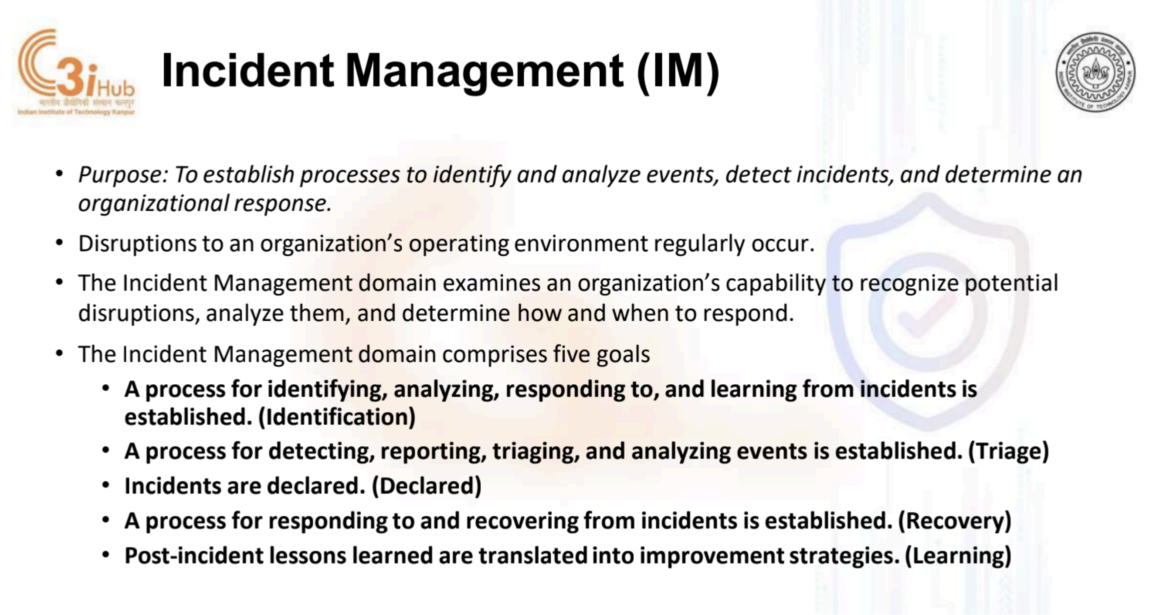
But sometimes the vulnerability patch is not yet available. you have to do something for the meantime right. So for the meantime you have to do some mitigation measures so that the exposure of that vulnerability to attackers is reduced. and then eventually you have to also analyze the root cause right. So, why did that vulnerability happen and then the root cause has to be addressed. Now in some cases the vulnerability is just a technological vulnerability like the XZ vulnerability, but remember the root cause is not technology root cause is actually dependence on open source software which is basically a supply chain security problem right.

So, the supply chain has been compromised. So, the root cause is that we are not checking the risks that are coming from the supply chain side. So, that is where the root cause has to be analyzed. So, vulnerability management has to be practiced for each of these goals. You can look at them and see whether it makes sense. Then there is incident management and there is service continuity management.



Service Continuity Management (SCM)

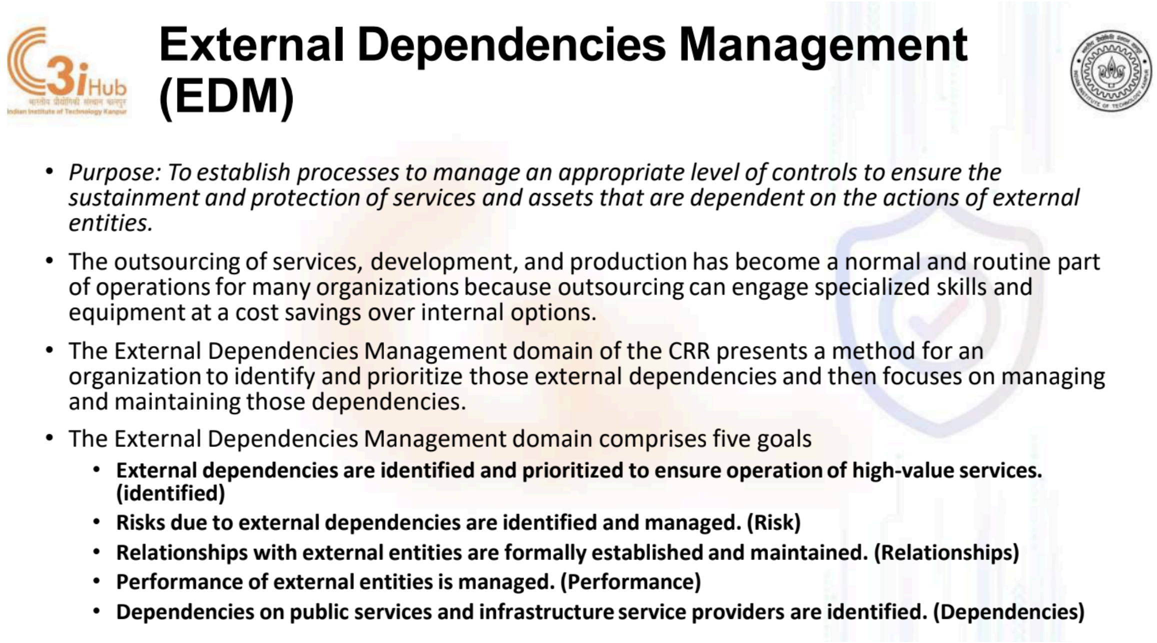
- *Purpose: To ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other event.*
- The process of assessing, prioritizing, planning and responding to, and improving plans to address disruptive events is known as service continuity.
- The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of the critical services.
- The Service Continuity Management domain comprises four goals
  - **Service continuity plans for high-value services are developed. (high-value)**
  - **Service continuity plans are reviewed to resolve conflicts between plans. (Conflict Resolved)**
  - **Service continuity plans are tested to ensure they meet their stated objectives. (Tested)**
  - **Service continuity plans are executed and reviewed. (Reviewed)**



Incident Management (IM)

- *Purpose: To establish processes to identify and analyze events, detect incidents, and determine an organizational response.*
- Disruptions to an organization's operating environment regularly occur.
- The Incident Management domain examines an organization's capability to recognize potential disruptions, analyze them, and determine how and when to respond.
- The Incident Management domain comprises five goals
  - **A process for identifying, analyzing, responding to, and learning from incidents is established. (Identification)**
  - **A process for detecting, reporting, triaging, and analyzing events is established. (Triage)**
  - **Incidents are declared. (Declared)**
  - **A process for responding to and recovering from incidents is established. (Recovery)**
  - **Post-incident lessons learned are translated into improvement strategies. (Learning)**

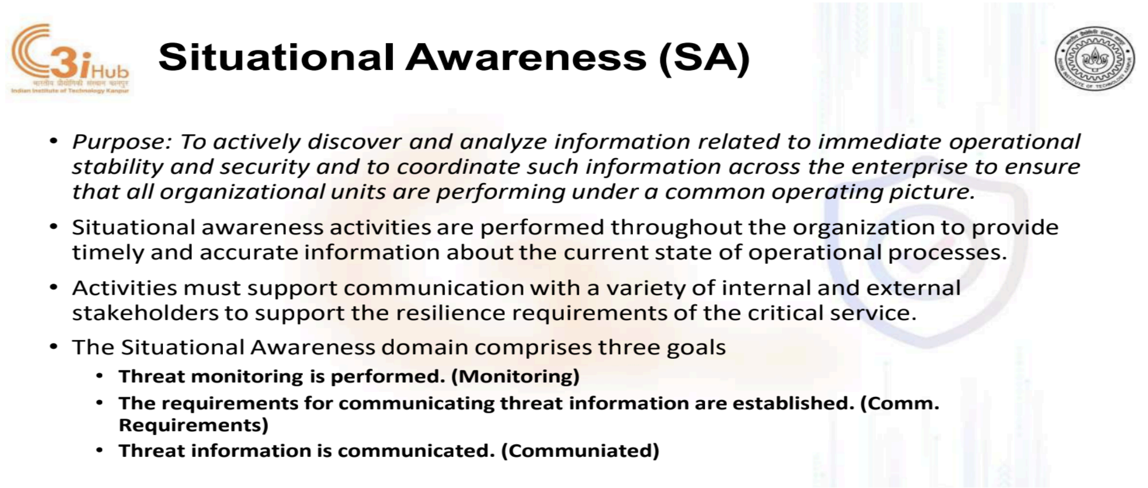
This is very important for resilience or business continuity management, risk management. and this is the external dependency management this is where the supply chain management comes right. We have a lot of dependencies on external software as well as external people. We often have vendors who give VPN access to the vendors into our critical servers to fix the server or to configure the server to upgrade the server or you know do other things. And, this is what was used in the Ukraine power system attack for the first time in 2015. When VPN access was stolen VPN access credentials were stolen and then they got VPN access to the critical infrastructure, where they could basically control the breakers to stop the power flow right.



External Dependencies Management (EDM)

- *Purpose: To establish processes to manage an appropriate level of controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external entities.*
- The outsourcing of services, development, and production has become a normal and routine part of operations for many organizations because outsourcing can engage specialized skills and equipment at a cost savings over internal options.
- The External Dependencies Management domain of the CRR presents a method for an organization to identify and prioritize those external dependencies and then focuses on managing and maintaining those dependencies.
- The External Dependencies Management domain comprises five goals
  - **External dependencies are identified and prioritized to ensure operation of high-value services. (identified)**
  - **Risks due to external dependencies are identified and managed. (Risk)**
  - **Relationships with external entities are formally established and maintained. (Relationships)**
  - **Performance of external entities is managed. (Performance)**
  - **Dependencies on public services and infrastructure service providers are identified. (Dependencies)**

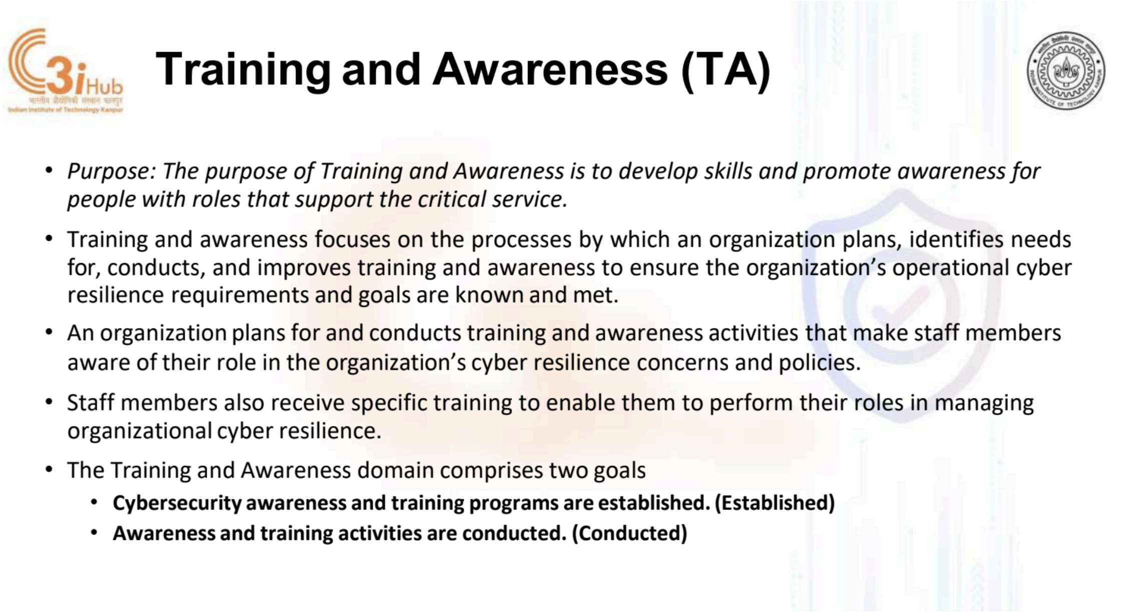
So, external dependencies are not only about a software bill of material based dependency, but also dependency on vendors and you know giving access to vendors and things like that. and then the final I think not the final one but the ninth is the training and awareness this is very important people process technology so there are two goals here awareness and training program has to be established and they have to be conducted right and



Situational Awareness (SA)

- *Purpose: To actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture.*
- Situational awareness activities are performed throughout the organization to provide timely and accurate information about the current state of operational processes.
- Activities must support communication with a variety of internal and external stakeholders to support the resilience requirements of the critical service.
- The Situational Awareness domain comprises three goals
  - **Threat monitoring is performed. (Monitoring)**
  - **The requirements for communicating threat information are established. (Comm. Requirements)**
  - **Threat information is communicated. (Communiated)**

then last one is situational awareness that is the SOC security operation center security incident and event management system having intrusion detection, network intrusion detection having endpoint intrusion detection and so on. So, situational awareness is very important. So, you read this up to this point. I will talk a little bit about the maturity indicator levels and how this model measures maturity. The reason I want to go through that a little bit is because it will give you an idea like in the future if you are looking at any kind of maturity model like a beta software make capability maturity like CMM or you are looking at C2M2 that is the cyber security maturity model or resilience maturity model.



Training and Awareness (TA)

- *Purpose: The purpose of Training and Awareness is to develop skills and promote awareness for people with roles that support the critical service.*
- Training and awareness focuses on the processes by which an organization plans, identifies needs for, conducts, and improves training and awareness to ensure the organization’s operational cyber resilience requirements and goals are known and met.
- An organization plans for and conducts training and awareness activities that make staff members aware of their role in the organization’s cyber resilience concerns and policies.
- Staff members also receive specific training to enable them to perform their roles in managing organizational cyber resilience.
- The Training and Awareness domain comprises two goals
  - **Cybersecurity awareness and training programs are established. (Established)**
  - **Awareness and training activities are conducted. (Conducted)**

You have some idea about what do you mean by maturity model, how maturity is measured, what are the different progression of the maturity. Maturity the word maturity of course indicates you know a series of progression right because that is what maturity is all about. Like you initially you are low maturity and then gradually your maturity grows to a level where you have the highest level of maturity. So that's the kind of stuff I want to discuss. Then we will move on to the next topic right okay. Thank you.