**Practical Cyber Security for Cyber Security Practitioners**

**Prof. Sandeep Kumar Shukla**

**Department of Computer Science and Engineering**

**Indian Institute of Technology, Kanpur**

**Lecture 25**

All right. So, good morning. So, we were talking about the cyber resilience review. What I want to do first today is actually show you a cyber resilience review we did for IIT Kanpur in the previous version of this class, where the class was divided into 10 groups. Each group did one of the domains, right? The way it worked is that they went to CC, or actually, they sent the questions to CC, and they got responses. Based on the responses, they made their choices, and then some result came out. If we do it today, ideally, I should have done it this time with you guys, but for some reason, things got a little bit delayed.


So, we do not have enough time to do it because it requires about one and a half months or so to complete. We cannot suddenly bombard the engineers, who are already very busy, with questions from 10 different groups, right? But anyway, I want to show you what we got—not to analyze what we got, but just to show you what it looks like to get a cyber resilience review. So, they have a redesigned PDF file that you can download. I have made it available on the class website, where you can actually fill in things. For example, you can see that we have these buttons which allow you to revise the

assessment or print the report. The report gets automatically generated by the program and the scripts embedded into the PDF.


So, what we see here is a kind of instruction. This is what we call a self-assessment report. There are two ways to do this report. One is self-assessment, where the organization itself does the assessment after studying the goals and practices in each domain, understanding them, and then asking the relevant stakeholders within the organization about how well those practices are being implemented, etc.

The second way is to conduct what is called a facilitated assessment, where somebody from Homeland Security will come to your organization. You will have an all-day or couple-of-days workshop where all the stakeholders will be present, and the facilitators will actually explain each question and ask you for the answers. As stakeholders who know about what is being done currently, you will talk about that, right? This was done in November 2022. This table of contents is auto-generated. This is some DHS notification. This is the overview and scope.


# CYBER RESILIENCE REVIEW

# SELF-ASSESSMENT REPORT

## FOR

## Computer Centre, IIT Kanpur

November 17, 2022

### Table of Contents

## Notification

*This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.*

*The DHS does not endorse any commercial product or service, including the subject of the analysis in this report. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.*

*The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.*

## Cyber Resilience Review Report for

Computer Centre, IIT Kanpur

### Introduction

On November 17, 2022, Computer Centre, IIT Kanpur conducted a Cyber Resilience Review (CRR) Self-Assessment. Answers to questions about cybersecurity practices were gathered from key stakeholders within Computer Centre, IIT Kanpur and scored.

As we will see, it is very important to decide the scope. For example, if you are a bank, the bank has many critical business processes. One is to, for example, give out loans—loan processing. Another critical function is to enable payments. People make payments using checks, NEFT, IMPS, RTGS, UPI, maybe a RuPay credit card, and so on.

### Overview and Scope of the CRR

The CRR consists of a one-day, structured facilitation and interview of key personnel. The primary goal of the CRR is to develop an understanding and qualitative measurement of essential cybersecurity capabilities. Personnel are asked to describe how these capabilities are institutionalized and managed, and how these capabilities are applied to support the organization during times of stress. The assessment questions asked participants to articulate evidence regarding both performances of cybersecurity practices as well as sustainment of those practices over time. Individual organizations are examined for specific capacities and capabilities in defining, managing, and measuring cybersecurity practices and behaviors, as described in categories. The categories examined are:

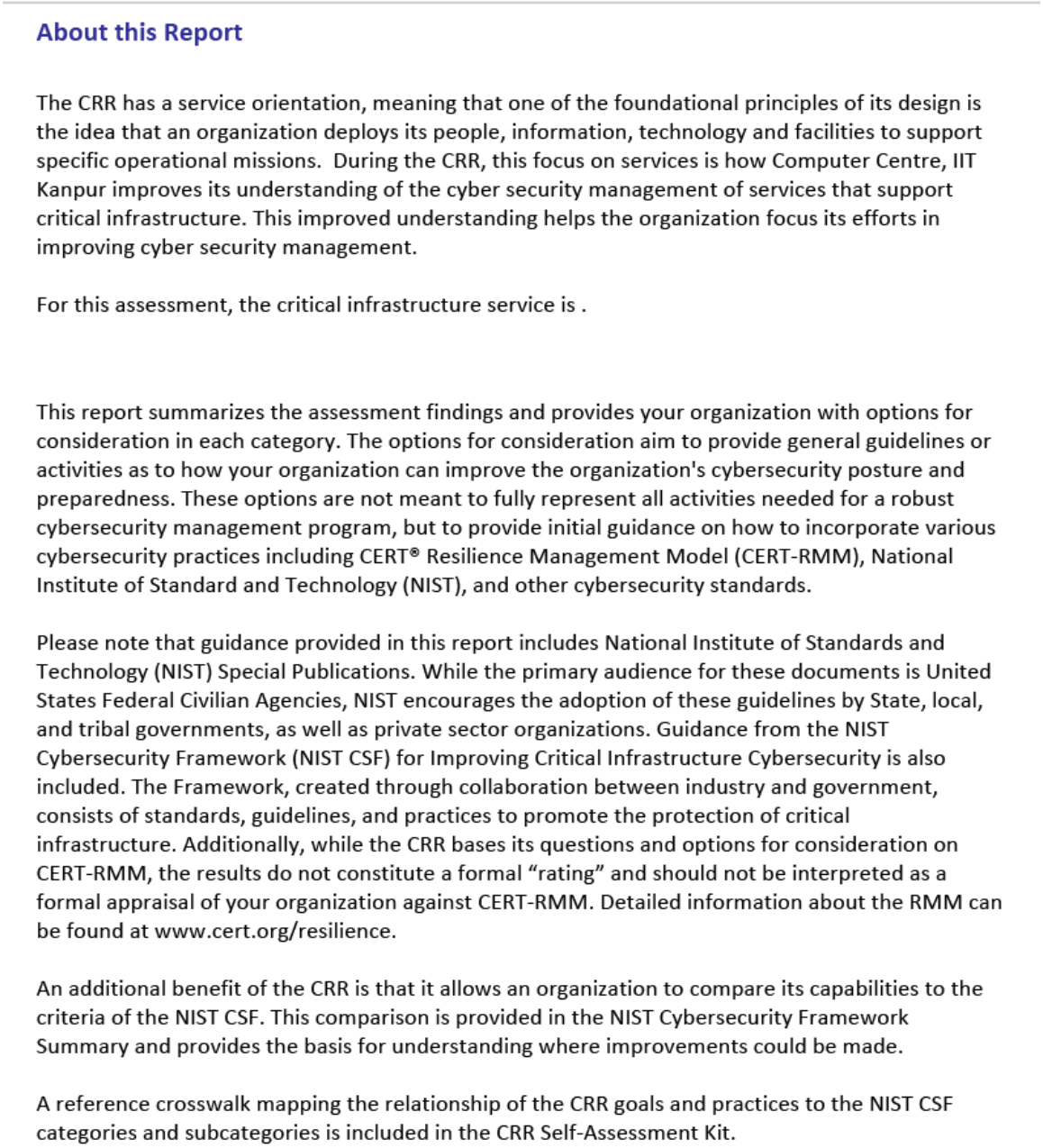
1 Asset Management
2 Controls Management
3 Configuration and Change Management
4 Vulnerability Management
5 Incident Management
6 Service Continuity Management
7 Risk Management
8 External Dependencies Management
9 Training and Awareness
10 Situational Awareness

The categories examined are derived from a larger security and business continuity framework known as the CERT® Resilience Management Model (CERT-RMM), which was developed by the CERT Program at Carnegie Mellon University's Software Engineering Institute.

All these things are different business processes, and for each of these, there are certain goals in terms of service. For example, RBI requires that your mean downtime per month should be no more than a certain number of minutes for the payment system, or your time to recovery, if it goes down, should be no more than a certain number. If it does exceed that RBI stipulation, then they have to answer to RBI as to why they exceeded the stipulated time frame, right? The same thing applies to loan processing. There are certain goals, for example, how fast a decision must be made between the application and a decision, what risk level you are allowed to take, and what should be the goal for your non-performing loans—that is, loans that are unlikely to come back, etc.

So, each function of an organization will have different sets of goals. So now, in an academic institute, for example, we have a lot of important functions, such as the registration process, right, even though the registration process is only in effect at certain times, right? So, certain time windows it's in effect, but during the registration time, we don't want the registration process to shut down or crash. We don't want the registration process to make any mistakes in terms of assigning courses—you know, the one that you

apply for versus the one that you actually are assigned. So, there are certain goals that have to be set.



## About this Report

The CRR has a service orientation, meaning that one of the foundational principles of its design is the idea that an organization deploys its people, information, technology and facilities to support specific operational missions. During the CRR, this focus on services is how Computer Centre, IIT Kanpur improves its understanding of the cyber security management of services that support critical infrastructure. This improved understanding helps the organization focus its efforts in improving cyber security management.

For this assessment, the critical infrastructure service is .

This report summarizes the assessment findings and provides your organization with options for consideration in each category. The options for consideration aim to provide general guidelines or activities as to how your organization can improve the organization's cybersecurity posture and preparedness. These options are not meant to fully represent all activities needed for a robust cybersecurity management program, but to provide initial guidance on how to incorporate various cybersecurity practices including CERT® Resilience Management Model (CERT-RMM), National Institute of Standard and Technology (NIST), and other cybersecurity standards.

Please note that guidance provided in this report includes National Institute of Standards and Technology (NIST) Special Publications. While the primary audience for these documents is United States Federal Civilian Agencies, NIST encourages the adoption of these guidelines by State, local, and tribal governments, as well as private sector organizations. Guidance from the NIST Cybersecurity Framework (NIST CSF) for Improving Critical Infrastructure Cybersecurity is also included. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. Additionally, while the CRR bases its questions and options for consideration on CERT-RMM, the results do not constitute a formal “rating” and should not be interpreted as a formal appraisal of your organization against CERT-RMM. Detailed information about the RMM can be found at www.cert.org/resilience.

An additional benefit of the CRR is that it allows an organization to compare its capabilities to the criteria of the NIST CSF. This comparison is provided in the NIST Cybersecurity Framework Summary and provides the basis for understanding where improvements could be made.

A reference crosswalk mapping the relationship of the CRR goals and practices to the NIST CSF categories and subcategories is included in the CRR Self-Assessment Kit.

Now, when these goals are set, only then can you think about cybersecurity, right? Because if there is no goal set, what is this... of course, there's also the data security, data privacy issue—you don't want, at any cost, any data to be leaked, right? So that's irrespective of, you know, what business it is. Anytime there's personally identifiable information, you don't want that to be leaked. And today in India, we have the Data Privacy Act passed. It has not been notified yet, but once it is in effect, then it may cost...

according to the new law, the DPDP Act, it will be up to 250 crores penalty per time this breach happens. Plus, the affected individuals can also sue the company, and so on.

### Cyber Resilience Review Results

The CRR is an interview-based assessment. It is understood that participants often do not have complete knowledge of an organization's operations. Actual performance may vary from what is indicated in this report. Organizational performance is presented across several dimensions within the report. Scores are provided for individual Practices, Goals, and Domains.

### Basic Rules

1. Practices are either performed (answer ="Yes"), incompletely performed (answer = "Incomplete"), or not performed (answer = "No")

2. A goal is achieved only if all practices are performed

3. A Domain is achieved at MIL-1 if all the Goals in the Domain are achieved

4. A Domain can be achieved at higher levels if the MIL questions for each level (MIL-2 through MIL-5) are answered.

### Scoring Rubric

***Step 1***

Each Practice in a Domain is scored as the following:

- performed when the question is answered with a "Yes" (green)
- not performed when a question is answered with an "Incomplete" (yellow) or "No" (red) or "Not Answered" (grey)
- if "Not Answered" (grey) is shown, the question was left blank and is scored the same as a "No"

***Step 2***

Each Goal within the Domain is then scored as the following:

- achieved when all practices are performed (green)
- partially achieved when some practices are performed (yellow)
- not achieved when no practices are performed (red)

***Step 3***

Each Domain is assigned a MIL level based on the following:

- MIL-0 if only some of the goals are achieved
- MIL-1 if all of the goals are achieved
- MIL-2 if MIL-1 is achieved and all of the MIL-2 questions are answered YES
- MIL-3 if MIL-2 is achieved and all of the MIL-3 questions are answered YES
- MIL-4 if MIL-3 is achieved and all of the MIL-4 questions are answered YES
- MIL-5 if MIL-4 is achieved and all of the MIL-5 questions are answered YES

So that's separate, like the privacy and data confidentiality, but other than that, to get the businesses actually meeting their business goals, one has to actually then think about what are the risks to not achieving their goals. Each business process may have multiple different goals, and you have to see what are the risks that will stop me from achieving my goals. For example, in the case of a payment system, if it's like 30 minutes per month that I can be down, then what are the risks, right? And among many risks, there would be a risk about cyber, right? So not every risk is related to cyber. For example, there may be

a risk where, you know, the system may crash, right, just because it has become an old server or something.

Or the server has some manufacturing defect. So, do we have, you know, a backup server, you know, live standby, so that if one crashes, the other can take over within seconds, and all that stuff? So those are risk mitigations, which are unrelated to cyber attack-related risks. So, what we are doing here is saying that, among all the risks, assuming that all the other risks are taken care of, if I have this cyber risk and I get attacked, and I get affected, then am I going to be able to still provide service and recover to normal service quality as soon as possible? And that mean time to recover, or mean time to perform, may actually be also part of the business goals, right? I may want to recover within maybe 30 minutes or 1 hour, whatever.

So here, the question is, what is the scope? So, while this was done, the scope was not very well defined. So we have multiple different businesses. For example, we have... not businesses, but business processes. Like registration is one, payroll is another, Dean R&D office automation is another. There could be automation of the gates through which cars come into the campus. That is also an automated computerized system. You have power generation, power transmission, or sorry, power distribution plants, substations at various locations on the campus. Those are also possible things, and sewage control, water pumping, and all that stuff. All that stuff are business processes. Now, the question is, what is critical for this organization? This organization now... who will decide what is critical, right? So, the board of governors will determine what is critical. You and I cannot determine. Like, for example, as a resident of the campus, if water doesn't come, I get really, you know, inconvenienced, and therefore I could say that that is critical, right?

But actually, what is the business this organization is into? And that is the education and research business, and therefore, the criticality will be determined by that. Like, is it that we wouldn't be able to run courses? Or we wouldn't be able to do registration during the registration period? Or you wouldn't be able to process payroll payments during the payment cycle, and things like that, right? Whether, you know, the research expenditure, etc., cannot be done because office automation is not working. Or the email system—the email system is very important for an academic institute to run. The email system may actually get broken by a cyber attack, or the email system may actually be used to spoof the users and then get into bigger, you know, cyber attacks, and so on. So, all these things you have to decide: what scope in which you are trying to determine the resilience. Similarly, you can also do organizational scope.

So, you do not necessarily have to do the scoping based on service. So, you can say I want to see these two services the resilience of these two services other services I do not

care if it is resilient as long as it is more or less resilient. So, I may not do this kind of minute analysis. But, on the another way to do this is to you know organizational scope for example, I can decide that only the office automation is what I am you know I want to do or I want to only do computer science department right. So, I want to do the resilience of computer science department.

Because, computer science guys are you know asking for it right. So, that is the kind of scoping has to be done. In this case what happened is the scoping was done for everything right. So, almost like email to you know office automation to Pingla to you know payroll system accounting system all that stuff right. So, this is little bit of from you know.

So, you know if you include everything in the scope like it is likely that your maturity will be very low because there will be some service in which the maturity is not very good, but you get the lowest of the of all right your maturity level will be given the lowest of all the all the maturity levels for all the services right. So here you will see that the maturity level that came out is actually not very high it was it was one maturity level out of you know five different maturity levels we will see what the results are and then we already have seen that these are the these are the domains in which I want to do this maturity assessment. So this is the report writer, so this team that worked on this. So I basically made actually 11 teams. So 10 teams were actually doing filling out the assessment for 10 domains and then they were sending it to the last team and the last team was putting it together right.

So they did the final report generation and writing all this basic stuff. So scoring is that every practice has three answers possibly yes we are performing this practice or I am performing but not to the fullest extent possible so incomplete or no means that this is not being done. not answered is gray and not answered is not going to help much in terms of you know it might as well be red right if you are not answered you assume that it is not being done. So for every practice we say that it is green when each domain so this is for individual practice. So individual practices can be eventually be colored green, yellow, red or gray and then you can say that for the overall domain what is the overall domains performance it has to see if all practices are performed then only the domain gets green.

Even if you miss one practice out of let us say 15 practices for that domain then you cannot get green. when some practices are performed, so yellow, so if even if you miss one you will get yellow and if no practices are performed then it is red right, so it is red means really bad no practice is being performed. And then each there is also a maturity level, so practices are performed or not performed or you know semi-performed right. But domains then domains become that based on whether all practices are performed or

some practices are performed or no practices are performed. But the maturity level is how the practices are implemented right.

### Maturity Indicator Levels

Maturity Indicator Levels (MIL) are assigned by Domain and represent a consolidated view of performance. CERT-RMM MILs describe attributes that would be indicative of mature capabilities as represented in the model's capability levels. However, they do not fully represent capability levels as defined because a capability level can only be assigned through a formal appraisal process, not as the result of using an assessment-based instrument.

***MIL0 Incomplete***

Indicates that Practices in the Domain are not being performed as measured by responses to the relevant CRR questions. If MIL0 is assigned, no further assessment of maturity indicator is performed.

***MIL1 Performed***

Indicates that all Practices in a Domain are being performed as measured by responses to the relevant CRR questions. MIL1 means that there is sufficient and substantial support for the existence of the practices.

***MIL2 Planned***

Indicates that all Practices in Domain are not only performed, but are supported by sufficient planning, stakeholders, and relevant standards and guidelines. A planned process/practice is

- established by the organization (Is the practice documented and communicable to all who need to know?)
- planned (Is the practice performed according to a documented plan?)
- supported by stakeholders (Are the stakeholders of the practice known and are they aware of the practice and their role in the practice?)
- supported by relevant standards and guidelines (Have the standards and guidelines that support the practice been identified and implemented?)

So MIL 0 really bad only some goals are achieved right, so MIL 0 means that there are domains for each domain. There are some practices or some goals for which actually you know all practices are achieved, if all goals are achieved for a particular domain then that means that all practices are being done then I get MIL 1. So, for a domain let us say there are 5 goals and let us say there are 20 practices across all the goals if I do I am doing all the practices that is all the practices are green then that particular goal will be achieved and then if all goals are achieved for a particular domain then we will say it is in the first maturity level. Then if I want to see, if I want to be better than first maturity level then I have to not only get all the mil one that is I have to get all the goals achieved but then there are specific things that I have to do and we will go into that what specific things have to be done then so this becomes cumulative that is to get to MIL 3 you have to satisfy MIL 1 and all answers of MIL 2 and all other answers of MIL 3 right and so on so forth so this is how the maturity progresses. So there are specific names also to remember what each maturity level indicate.

So, remember the maturity is about progression in some sense right. So, higher maturity means I have progressed beyond the previous maturity level right. So, that is the idea. So, you see that MIL 0 means incomplete that is some goals are not achieved right in a domain in domain is considered incomplete if the in domain that domain some goals are not achieved. Now if all goals are achieved in a particular domain then we say that that domain is performed that is I am performing the practices as required to achieve the goals.

Now MIL 2 is called planned. So remember that we said that in MIL 2 what we did is that if to get to MIL 2 I have answer certain questions on top of MIL1 right MIL1 means performed and then some additional questions so what are those questions this here you will get the hints of what questions are being asked so we are saying that okay you are performing everything but Have you documented the practices and communicated to all who need to know? See one of the biggest concern that we see in like we have done for example many ports audit right cyber audit. We find that depending on who is the CISO, who is the chairman, who is the IT in charge, etc., the practices vary, right. But that should not be the case, right. So all the ports should have same kind of cybersecurity practices being performed.

So unless it is documented and communicated, it is communicable. then you cannot replicate elsewhere right because you then you have to really bring the actual person who is doing in one place to bring that person there and ask him to work again from scratch to get that place bring to the same maturity level that is not practical right. So, therefore, I have to make sure that the person it is documented and communicable. So, it can be replicated elsewhere then we are asking like whether there is a plan as to how the practice is performed. So it is not like I am you know because I know something, I know how to do this practice but if I leave then this practice cannot be done by the other people.

So there has to be a documented plan. and it has to be supported by stakeholders that is the do we know for each practice who are the stakeholders. In some cases the stakeholder could be the CISO, in some cases the stakeholder could be some IT people who are managing the assets and services, it could be also users like people who will not bypass you know authentication and things like that and are they aware of the practice and their role in the practice. So, this has to be properly documented and then it should be supported by relevant standards and guidelines. So I do not make practices out of thin air I do not say okay this from tomorrow this will be the you have to do this you have to do two factor authentication or we have to do you know endpoint security solution agents on every machine it has to be supported by standards such as 27001 or guidelines like NIST guideline or RBI guideline or SEBI guideline or some other certain guideline and so on.

So, it has to have that support. So, if you have all this in additional to the fact that you are doing the practices then you can get to MIL 2 that is a planned you are in a planned maturity. Then the next one is the managed to be managed you have to do all the practices plus you everything has to be documented plans stakeholder communicator and so on. On top of that this particular maturity level talks about governance. So, is the practice supported by policy and appropriate oversight over performance of the practice. So see the difference here and this is important to understand here we are saying that the practice is documented and communicable right I am not saying that the so say here it is still kind of dependent on the CISO and the team that is doing it.

They are basically documenting it and they are communicating it hopefully everybody is listening to the CISO and so on so therefore it is working out. But it is still not governed by the organization that is if this practice documentation is not kind of scripted into a policy. and when we use the word policy we use you know little bit more significance to the term policy because the policy a document does not become policy until it is adopted by the organization through its highest executive authorities right like the board of governors or board of directors they have to actually consider this and say that from now on we accept this as policy and therefore it is binding on everybody in the organization and if they are found to be you know in violation of any of the policy. then they will be subject to some penalty and that penalty may also be written into the policy that they may be suspend depending on the level of violation they may be fined suspended you know their increments may be reduced whatever right their appraisal may be affected whatever that should be in the policy. So that is the appropriate oversight over the performance of the practice, if any of the practices are not performed as per the policy, the policy should also state what would be the penalty and such things should be actually have legally binding that is if it is adopted by the board then it becomes within the organization the law right, it is a law of the organization it's appropriately stuffed and funded.

So, this is another thing. See here the CISO might say I am going to work 24 hours a day to make this all these practices work, I am going to work extra to make the documentation and so on and next CISO goes to another organization, new CISO comes, he says you know I am not going to do all this, I am going to take it easy. So therefore the organization should be properly staffed and funded. Otherwise if it depends on this factor that CISO has to do all this because there he does not have enough funding and staff then it is not unlikely to be sustained right. So it has to be sustainable by properly staffed and funded which means the top level CEO or such level have supported the cause, supported the cyber security cause or resilience is assigned staff who are responsible and accountable for the performance of the practice. So, there is you know it should not be like you know whoever is doing whatever right it has to be properly proper accountability should be there.

And then finally is you know are the staff adequately trained to perform the practice right. So this is the biggest hurdle nowadays because getting properly trained cyber security professional is very difficult and very expensive and therefore this is getting harder and now what has happened in India is that. So with NCIAPC with in a project with QCI Quality Council of India. they have not only come up with some policy guidelines for critical infrastructure, but they also have created a very elaborate requirements for what it means to be trained at what level, right. For what kind of job roles in the cyber security, what kind of training, what topics they have drilled down to the very topic level and that is a very important document that is that is going to be notified soon.

***MIL3 Managed***

Indicates that all Practices in a Domain are performed, planned, and have the basic infrastructure in place to support the process. A managed process/practice

- is governed by the organization (Is the practice supported by policy and is there appropriate oversight over the performance of the practice?)
- is appropriately staffed and funded (Are the staff and funds necessary to perform the practice as intended available?)
- is assigned to staff who are responsible and accountable for the performance of the practice (Have staff been assigned to perform the practice and are they responsible and accountable for the performance of the practice?)
- is performed by staff who are adequately trained to perform the practice (Are the staff who perform the practice adequately skilled and trained to perform the practice?)



- produces work products that are expected from performance of the practice and are placed under appropriate levels of configuration control (Does the practice produce artifacts and work products that are expected from performing the practice, and if so, are the configurations of these artifacts/work products managed?)
- is managed for risk (Are risks related to the performance of the practice identified, analyzed, disposed of, monitored, and controlled?)

So, hopefully it will be adopted by many organizations and there would be also training organizations that will come up. These training organizations will get accreditation from

QCI, Quality Council of India to train people according to this, right. So, that is the idea. So, anyway, so this is what it takes to be MIL-3. So, MIL-3 is beyond the fact that it is planned, but it is also governed by the organization with the organizational support at the highest level and with proper adequate staff and staff accountability and training.

***MIL4 Measured***

Indicates that all Practices in a Domain are performed, planned, managed, monitored, and controlled. A measured process/practice is

- periodically evaluated for effectiveness (Is the practice periodically reviewed to ensure that it is effective and producing intended results?)
- monitored and controlled (Are appropriate implementation and performance measures identified, applied, and analyzed?)
- objectively evaluated against its practice description and plan (Is the practice periodically evaluated to ensure that it adheres to the practice description and the plan for the practice?)
- periodically reviewed with higher-level management (Is higher-level management aware of any issues related to the performance of the practice?)

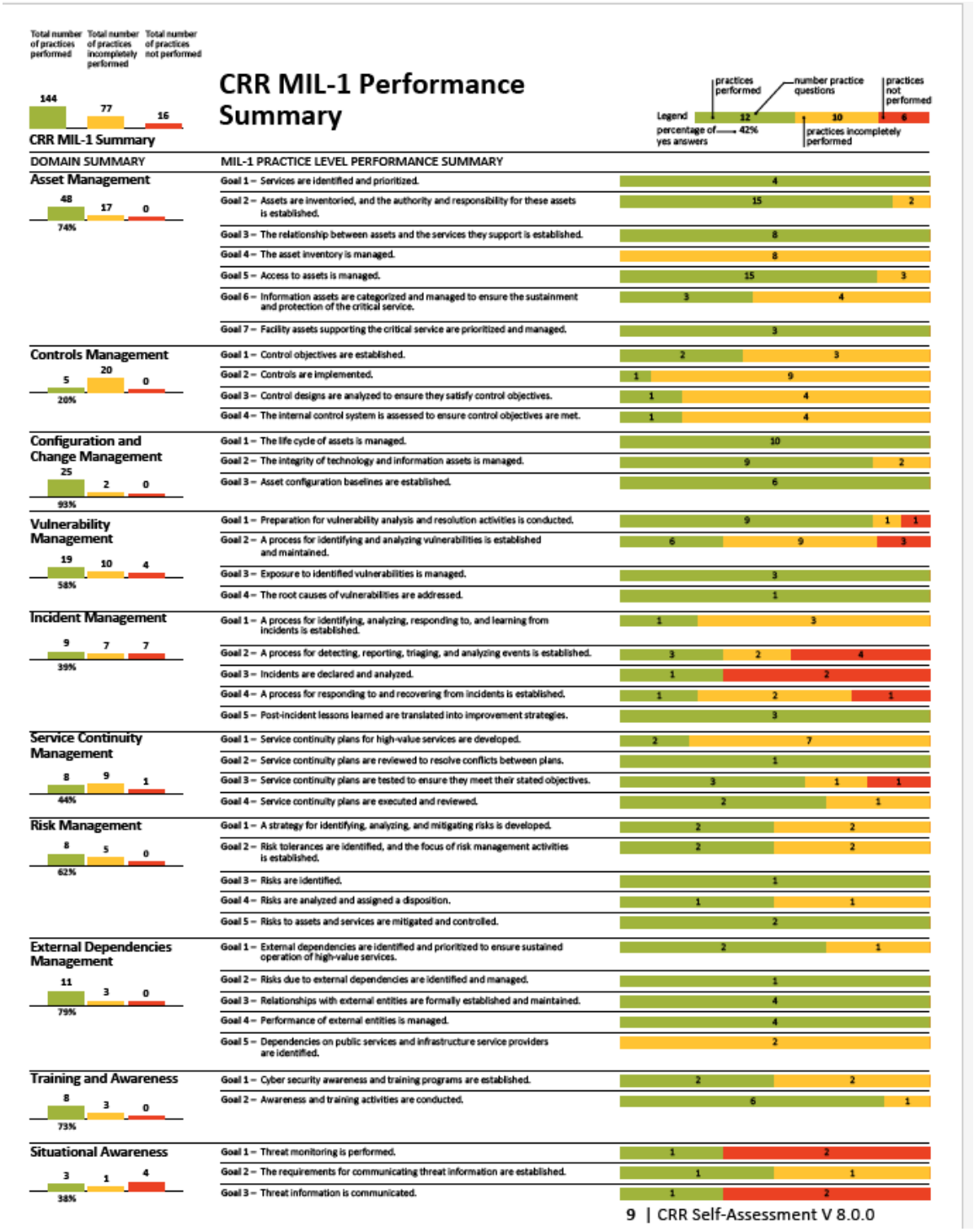
***MIL5 Defined***

Indicates that all Practices in a Domain are performed, planned, managed, monitored, controlled, and consistent across all internal[1] constituencies who have a vested interest in the performance of the practice. A defined process/practice ensures that the organization reaps the benefits of consistent performance of the practice across organizational units and that all organizational units can benefit from improvements realized in any organizational unit. At MIL5, a process/practice

- is defined by the organization and tailored by organizational units for their use (Is there an organization-sponsored definition of the practice from which organizational units can derive practices that fit their unique operating circumstances?)
- is supported by improvement information that is collected by and shared among organizational units for the overall benefit of the organization (Are practice improvements documented and shared across internal constituencies so that the organization as a whole reaps benefits from these improvements?)

[1] In this case, "internal" refers to constituencies over which the organization has direct managerial control.

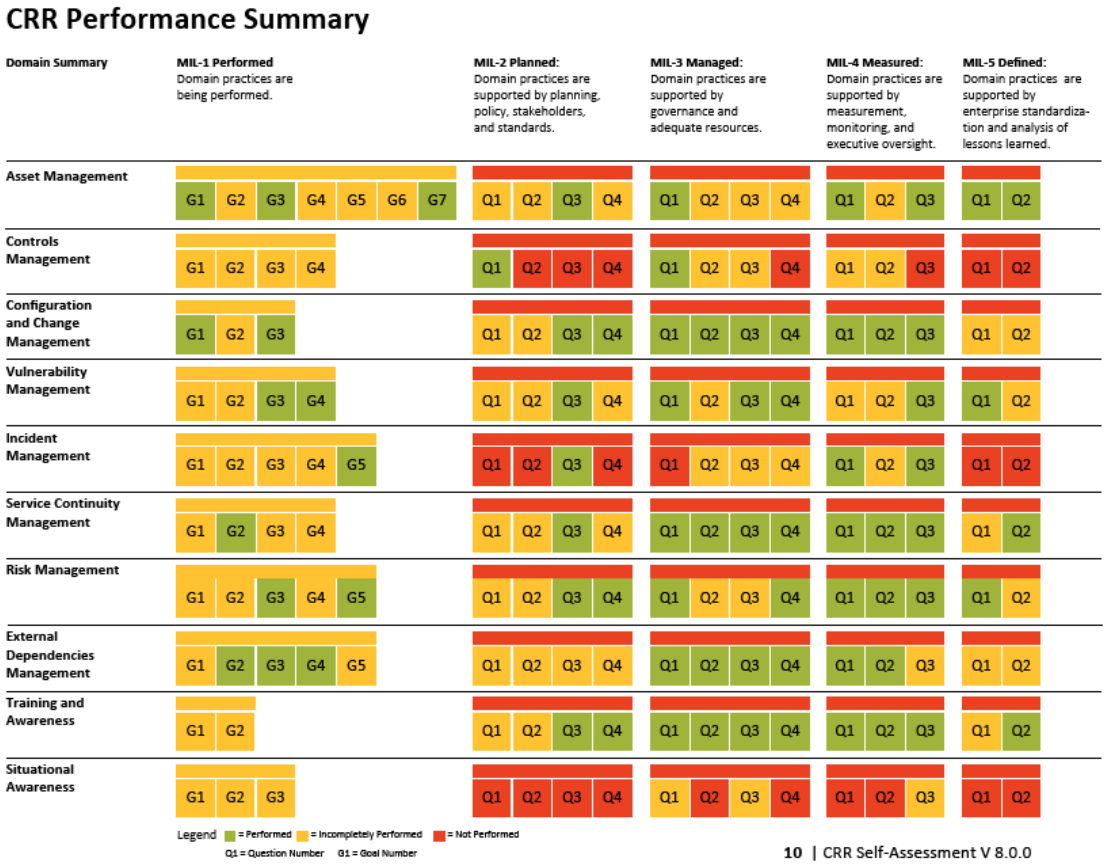
So that is the MIL-3. There is few more that periodically sorry is managed for risk. So risk assessment is properly performed and you know identified etcetera etcetera. Now next one MIL-4 is measured right. So yesterday the previous class I told you about this policy about procurement right and we said that the there is a elaborate documented communicated governed you know policy about procurement. but we do not measure it at least I am not aware that we measure its effectiveness right whether it actually produces what it is supposed to produce that is the price discovery.




So if you can say that all the practices are not only performed well planned managed governed and monitored and controlled. So, this monitoring and controlled is what comes here measured. So, periodically evaluated for effectiveness, monitored and controlled and objectively evaluated against its practice description and plan. and periodically reviewed with higher level of management. So, the CISO goes to the board

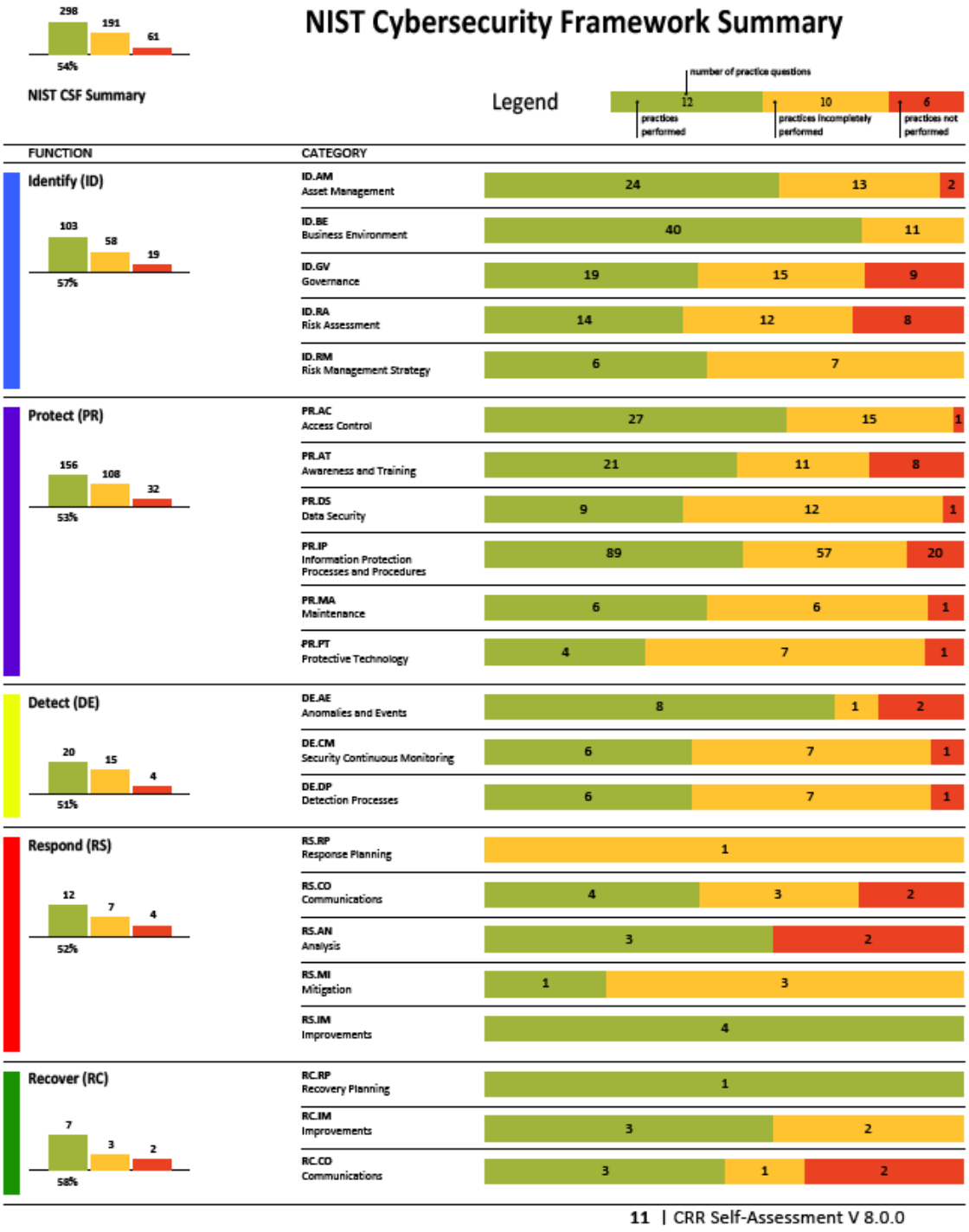
and says that here are the goals in this domain for this critical service and here is where we are and you know we may need to change something in our policy in our plans and you know or I may need more funding for more staff whatever.

So, that practice if that practice is periodic periodically reviewed with high level management then and the fact that you are actually evaluating its effectiveness then you are at the mill for that is measured. So the last the top most maturity level they are performed planned managed, monitored, controlled and now we are saying it is consistent across all internal constituencies who have vested interest in the performance of the practice. So this basically says that the same is replicated across the various units of the organization. So an organization may have multiple units. So it says defined by the organization and tailored by organizational units for their use and supported by improvement information collected by and shared among organizational units for overall benefit of the organization.




So different subgroups or subunits or whatever of the organization there has to be you know they should actually go by the same policy and same practices and plans. but they can tailor and then they should also any kind of improvement is made is then collected

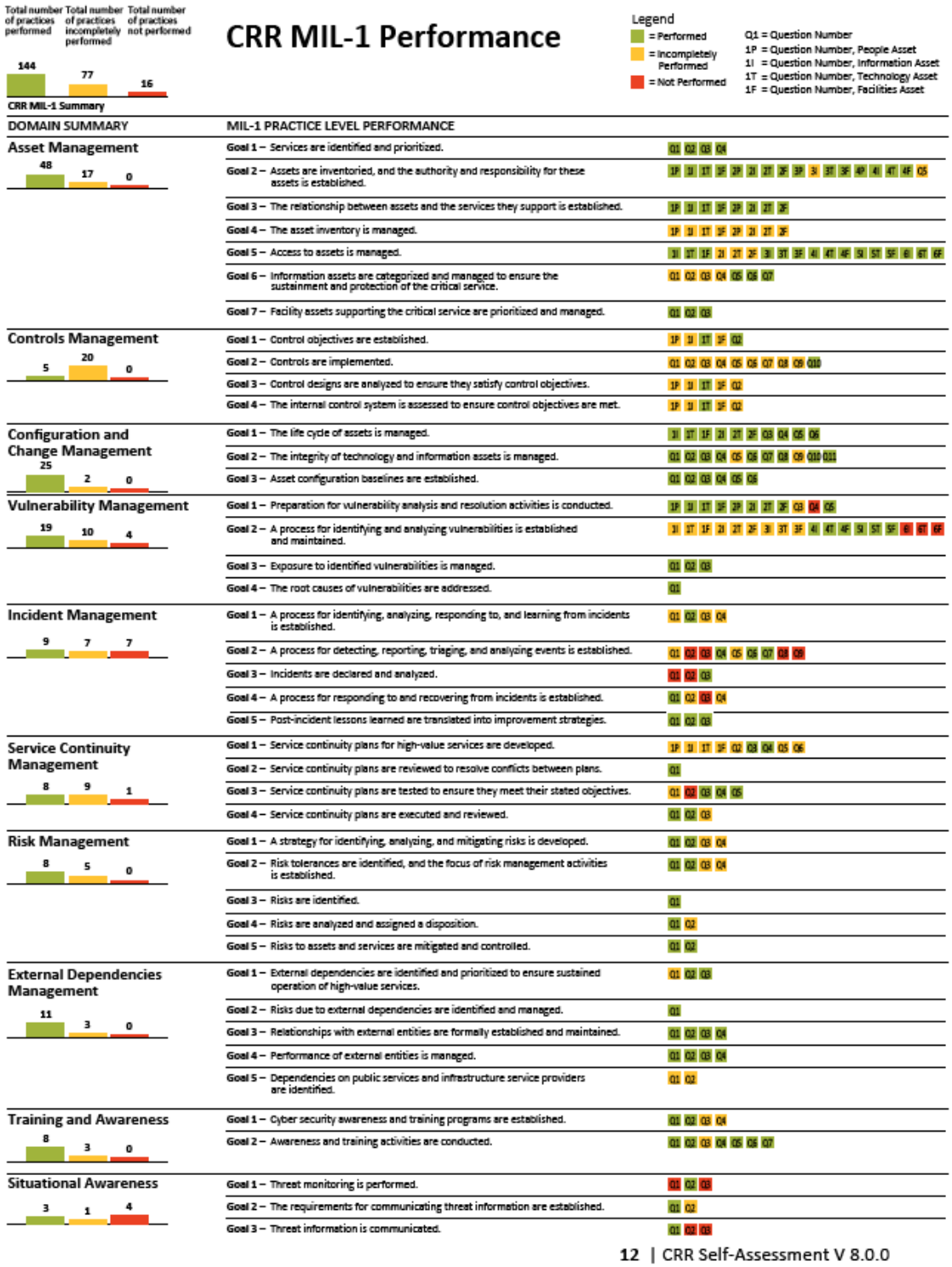
and shared among all the organizations so that everybody gets the benefit of this. So this is the fifth level of maturity.





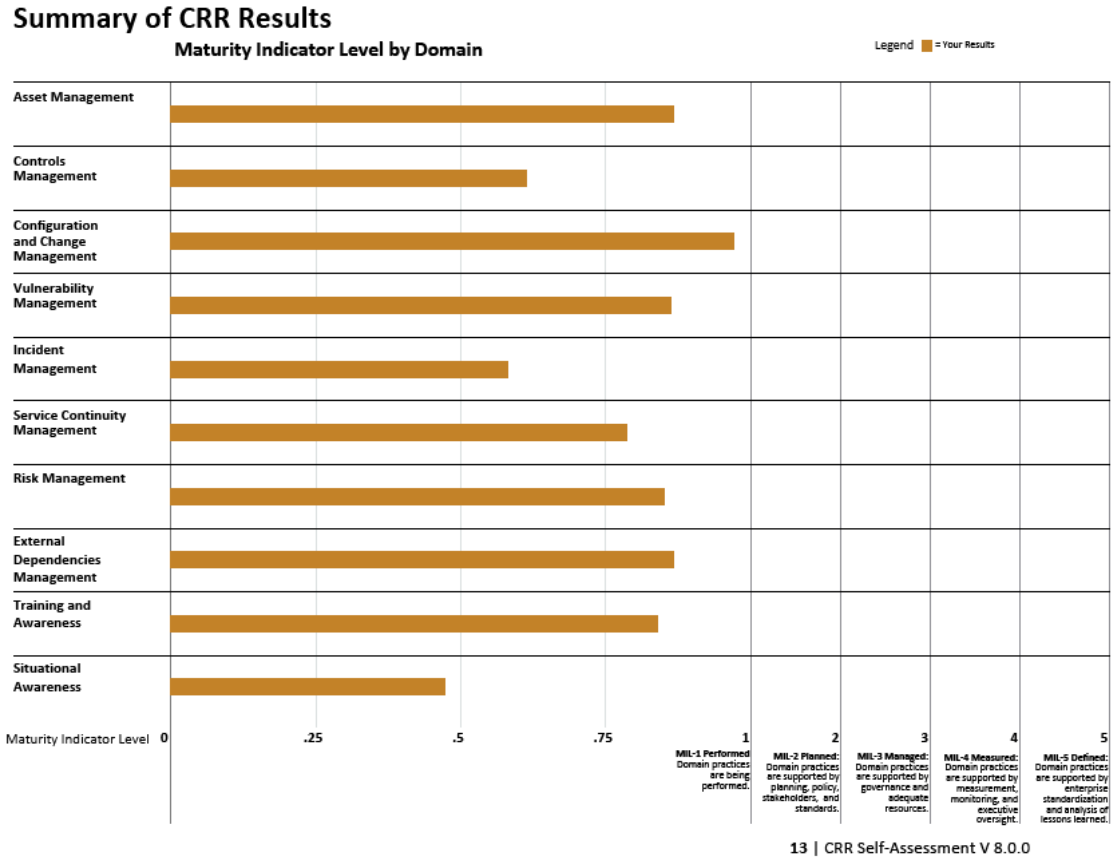

Now this is how the CRR decided or this is how the US you know RMM the Resiliency Maturity Model defines maturity it is you will if you read another maturity model like

C2M2 it is different it is not necessarily they are defined exactly in the same way, but usually they have a progression of different maturity levels. So now let us look at the actual thing that we went through last year, last to last year.




Here is the asset management. So remember asset management had 7 goals and in

November 2022, we found that services are identified and prioritized it is fully green I think which means all the practices for identifying which asset goes into which services cause all that stuff is done. Whereas assets are inventoried and authority and responsibility of these assets are established two practices seems to be incomplete yellow means incomplete means it is being done but not fully. The relationship between assets and services they support is established that seems to be fine. Asset inventory is managed. Now this asset inventory at that time if I remember correctly was a spreadsheet right.




So, spreadsheet cannot be easily managed right because it can be replicated. See if you have a database which is highly guarded and only people who are in charge of that database is allowed to update that database and so on, then it is can be managed. But if it is a if it is an excel sheet it can be copied around right. So, it is not managed and multiple copies means there will be inconsistency. Access to assets is managed, this is almost there, but there may seems to be some cases this is not proper, some practices seem to be missing and then information assets are categorized and managed like which one is critical, which one is not critical and so on.

So, that seems to be a little bit of lacking and the facility assets are prioritized and managed that seems to be fine. So you see the in asset management we are yellow because the domain will get the color that is the lowest color of all the different goals right. So then the next one is the control management. In control management, we seem to be not so good. So we have like out of four goals, none of the goals are fully green at that time and its majority incomplete, right.

So this is something that is of concern. In terms of the configuration and change management, it seems that life cycle of asset is managed, asset configuration baselines are established. This one I do not know if stick files and all are being used for benchmarking and or not, but at least that is what the collected data. Now remember each of these domains was done by different groups. and some groups are more serious they actually probed lot more than the other group like you know whatever right. So I am not I mean do not take this The evaluation results seriously right first of all it is old, second is that groups are groups were of different quality different training and all the stuff plus these are novice basically they are not like see they are not like homeland security cyber resilience experts.

So take it more like as an illustrative example and not exactly what the real situation is. Now then this is also yellow. This domain is also yellow. Now we have vulnerability management. Here we see that there are problem that we have reds now if we have reds that means that the entire thing become red right.

So now if we go further we have here I think service continuity management service oh so before that I think we missed something here which is. Incident after vulnerability we have incident management. Incident management is quite lacking here you know in terms of lot of red. So entire incident management gets red.

Service continuity management also for this small thing becomes red. And then we have the risk management, risk management is yellow and then I have you know external dependency management seems to be yellow as well and then awareness is yellow and situational awareness that we do not have a shock. So obviously situational awareness is low, so it will be red. Now what good is it? Note that I mean as I said repeatedly that do not take it they take it with a grain of salt about the real status of the situation but what it what good is such a you know if we assuming that it was done by real experts and assuming this is a true picture what can we say here. So here you see this is a low hanging fruit if I want to make this guy green. I can easily do this because I have only a little bit of practices that are incomplete.

Now, I have situational awareness I get the idea that it is in a real bad shape. So, I have

to do something about it, but it is not a low hanging fruit it probably will require a lot of activity budget buying expensive SOC and all that stuff and then if you look at this one this also requires a lot of work.

So, I will start with for example ... So I have to decide like which where I should start with so I would probably start with asset management and then I will also try to at the same time I try to fix this red and then this red and so on. So this will give you a picture of where we are and how to now go about approaching the you know better maturity so I actually see that we do not have a single goal which is green do we have so none of the domains are green. So now then the maturity level is actually 0 right now it also gives you more information. So in order to like in order to know the maturity questions, so those are questions about practices.

So for each of these there are also maturity questions. The questions for maturity level 1 and 2 and 3 and 4 are different and you see that in asset management we are not so bad in the sense that. we have now you see that this is red, this is red, this is red because I am not even at this maturity level so all these things are red by because I have to answer all this in green only then if I see here I am partially answering this to green and these are also partial but I am still red because in order to make this even yellow I need to get this as green. So, this gives you a very visual idea about where we are standing and where you know what where to start the improvement. So, this is you know the for each of these you know.

So, we see that you know where we are with respect to this questions. It also tells you in the NIST previous NIST 1.1 framework where we are with respect to what is my score. So NIST framework like remember we said NIST framework has identify, protect, detect, respond and recover right and now NIST 2.0 has governed also. So in each of these there are also subcategories like for example identification, asset management is part of the identification because you are identifying assets.

The business environment, you have to identify your business environment because that tells you what services are critical, what services are not critical and what is your threat environment and so on. In the previous version of NIST also governance was part of identification. risk assessment is part of identification and risk management strategy is another part of identification. So, in this we are seeing that we are actually you know how we are doing with respect to these sub sub categories of identify function. Clearly we are not fully doing identify function we are 57 percent into the identification function whereas in the protect we are at 53 percent.

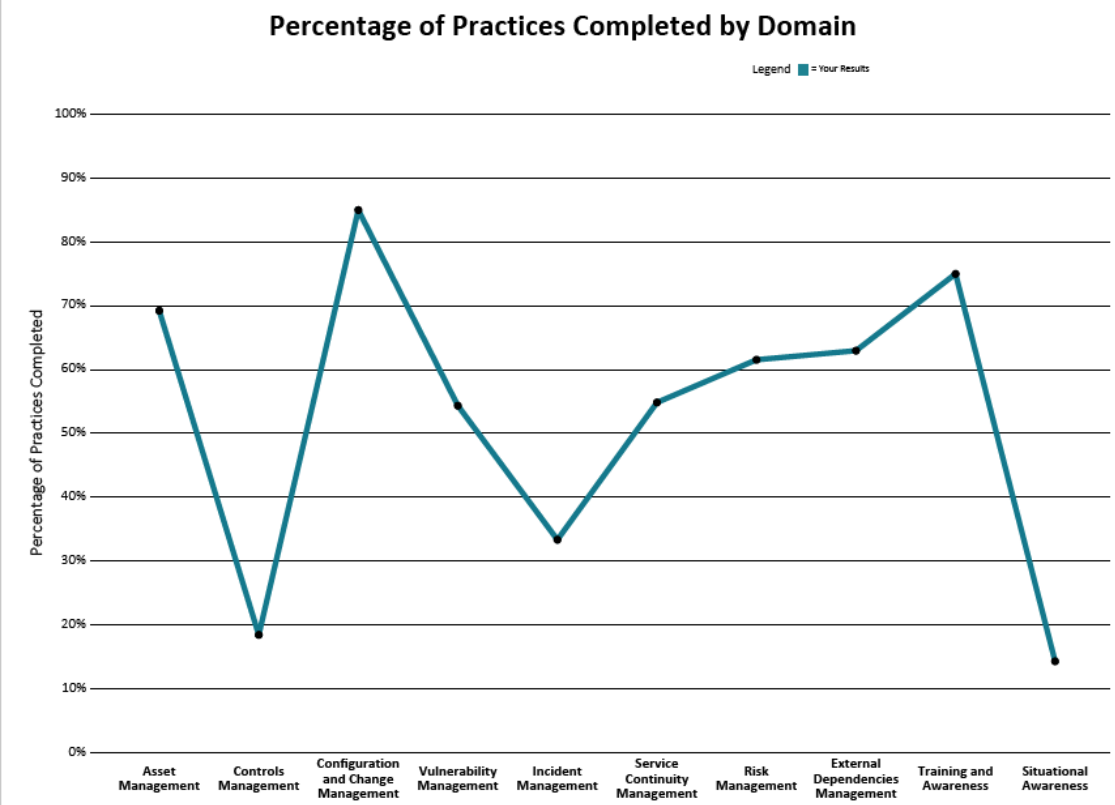
So, this numbers are not important what it is showing you is that by doing this evaluation

assessment you can actually get a rough approximate idea about where we are with respect to each of these. So, each of the NIST functionality. So, if you were like 100 percent in each of these then you could have said that you know I am NIST I am very NIST compliant I am NIST CSF compliant right. That is not that is a very tall order even the best banks probably will not get 100 percent in each of these, but they might get close.

So, that is where the NIST this thing. It also tells you you know the it gives you another view of you know which questions you are missing, which questions you answered partial, which questions you answered no, so that gives you a overall view. after assessment analysis by the CISO and his team or her team to decide how to go about fixing all this right whatever is missing so that. And they also have to make a goal right so for example some organizations they will say We will first fix the most critical ones, the ones that and then we will fix the ones that are less critical and so on. Some will say we will first fix low hanging fruits then the ones that will require a lot of investment and manpower etcetera expertise to fix so that kind of stuff.

So, you see this graph. so this graph is actually where you are with respect to the four domains this is the for the different mill so you are almost there if if mill one the one that is showing very poorly is situational awareness you are less than 50% in some of these you are almost there you are above three-fourth incident management also you are actually just like about 60% maybe 57, 56%. vulnerability management your configuration management you are doing almost there and asset management you are not too bad. So you have to use these graphs to decide how you are going to go about planning your next 3 months 6 months and so on and you have to present that to your top level executives to show you are and where you know where you want to be. So, you may actually draw this additional color here saying that where you will be in quarter and in the next quarter and where you will be in the next quarter and so on.

So, that you have a plan. So, this is another view of percentage of So, you see that in the controls management we are less than 20 percent, in the incident management we are less than 40 percent and in the situational awareness also we are less than 20 percent. So, these are some of the major concerns and this is the view that your board will like to see and you know and ask you that show me in the next quarter board meeting where you will be where you are. and at that time show this graph also if we see no improvement then we are going to you will lose your job. Unfortunately CISOs do not easily lose their job because I asked one of the board members of a bank and he said I can fire the CISO, but where will I get the next one right.




So, there is not enough well trained people for CISO. So, therefore, if you want to become a CISO you have a good chance you will make a lot of money except that it takes some time it may be may it may take you 10 years to become a CISO you would not get a CISO job right away unless it is a very small company, but the The CISO's job is to actually make this thing better to the level where all these things should be around here or maybe even higher, right. So that is where the visualization will help him to show that he is making progress, right. So this is further analysis of where these things are and so on.

We will not get into the details of that. But you get the idea. about where you know how these things work and since we did not get a chance for you to do this yourself, I just wanted to show you what it looks like if you do this. This is a pretty large document, but most of this is automatically filled by the script. See as you answered the questions everything else comes by automatically this is the beauty of this instrumentation of this PDF.

## 1 Asset Management

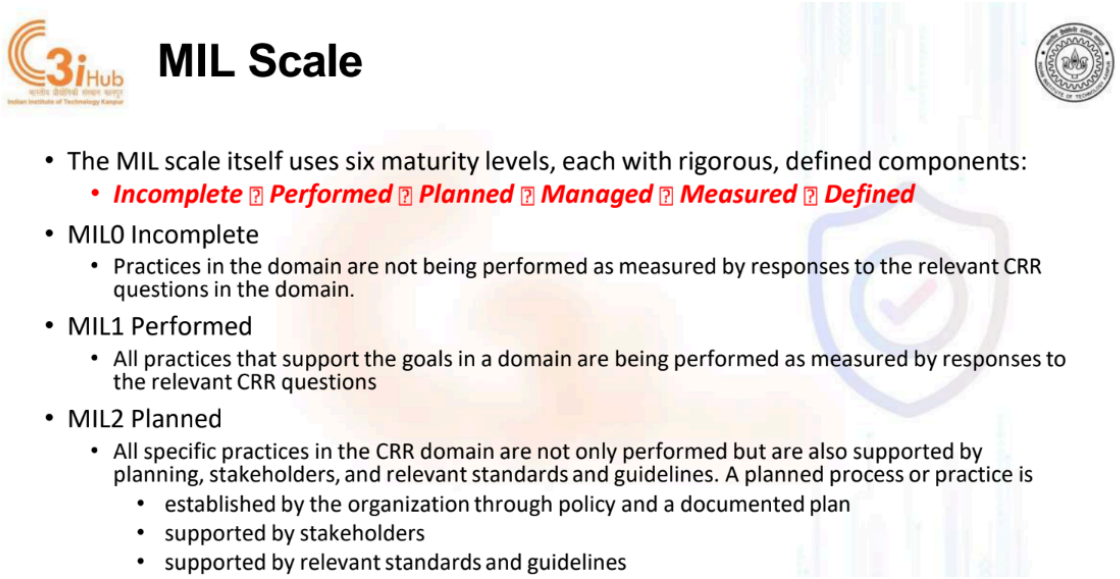

| | | |
|---|---|---|
| **Goal 1-Services are identified and prioritized.** | | |
| 1. | Are services identified? [SC:SG2.SP1] | Yes |
| 2. | Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1] | Yes |
| 3. | Is the organization's mission, vision, values, and purpose, including the organization's place in critical infrastructure, identified, and communicated? [EF:SG1.SP1] | Yes |
| 4. | Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP3] | Yes |
| **Option(s) for Consideration:** | | |
| Q1 | **CERT-RMM Reference**<br>**[SC:SG2.SP1]** Identify the organization's high-value services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission.<br><br>**Additional References**<br>Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 15-18<br><br>NIST CSF References: ID.BE | |
| Q2 | **CERT-RMM Reference**<br>**[SC:SG2.SP1]** Prioritize and document the list of high-value services that must be provided if a disruption occurs. Consideration of the consequences of the loss of high-value organizational services is typically performed as part of a business impact analysis. In addition, the consequences of risks to high-value services are identified and analyzed in risk assessment activities. The organization must consider this information when prioritizing high-value services.<br><br>**Additional References**<br>Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 16-18<br><br>NIST CSF References: ID.AM-5, ID.BE | |

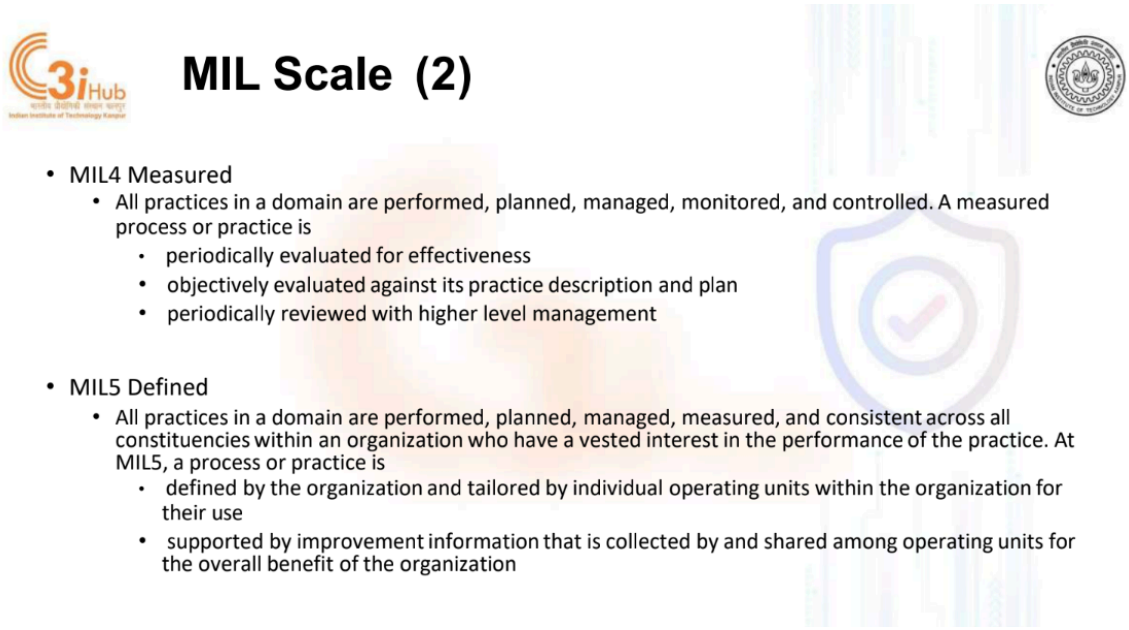
So, you do not have to do all this and you get something that you can show your management that this is where we are and then next time you do it you show where you are you show the two graphs side by side and that shows the progress you have made over a quarter or over two quarters whatever you are you have done. So that is that is where we are with respect to this with respect to this so I am not so I have slides discussing all this that I just discussed what are the different MIL scales you know incomplete performed planned managed measured and defined what they are and also how to do self-assessment you have to decide whether you are going to scope based on service or you want to scope based on organization.

| | | |
|---|---|---|
| Q3 | **CERT-RMM Reference**<br>**[EF:SG1.SP1]** Identify the organization's mission, vision, values, and purpose. From a resilience management perspective, the identification, comprehension, and communication of the organization's strategic objectives provides essential and necessary guidance and direction for the operational resilience management process. Effective operational resilience ensures that the organization can reach its strategic objectives.<br><br>**Additional References**<br>NIST SP 800-53 Rev. 4 PM-8<br><br>NIST CSF References: ID.BE-2 | |
| Q4 | **CERT-RMM Reference**<br>**[EF:SG1.SP3]** Prioritize and document the organizations strategic objectives. In order to appropriately scope the organization's operational resilience management process and corresponding operational resilience management activities, the high-value services of the organization that support the strategic objectives must be identified, prioritized, and communicated as a common target for success.<br><br>Affinity analysis between the organization's strategic objectives and services is a means to help the organization prioritize services and to identify high-value services that must be made resilient.<br><br>**Additional References**<br>NIST SP 800-53 Rev. 4 PM-11<br><br>NIST CSF References: ID.BE-3 | |
| **Goal 2-Assets are inventoried, and authority and responsibility for these assets is established.** | | |
| 1. | Are the assets that directly support the critical service inventoried (technology includes hardware, software, and external information systems)? [ADM:SG1.SP1] | |
| | People | Yes |
| | Information | Yes |
| | Technology | Yes |
| | Facilities | Yes |
| 2. | Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2] | |
| | People | Yes |
| | Information | Yes |
| | Technology | Yes |
| | Facilities | Yes |
| 3. | Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3] | |
| | People | Yes |
| | Information | Incomplete |
| | Technology | Yes |
| | Facilities | Yes |

And then you know what are the key roles like there would be a sponsor usually who would have a broad understanding and important of importance and components of the service for which the self-assessment is being done. So, usually it is the owner of that particular service. There would be a facilitator either from inside the organization or from that homeland security and then there would be subject matter experts will interpret the

questions for you because you may not even know what it means to do something like a asset you know assign or connect an asset to a particular service or what it means to do control you know defining the controls and so on so forth.




So you need subject matter experts then you basically decide who are the subject matter experts and participants for each of these domains not every domain the guys who are involved in an organization in asset management may not be doing risk management or incident management right.

# Attaining an MIL level

- In the progression of MILs, an organization can only attain a given MIL if it has attained all lower MILs.
- An organization that fails to perform all of the cybersecurity practices at MIL1 in a domain would also fail to reach MIL2 in that domain, even if it would have satisfied all the requirements at MIL2.

# Conducting Self Assessment

- Identifying the Scope of the Self-Assessment
- This scoping exercise is critical because answers to the self-assessment questions must be provided in relation to a specific service.
- The scope of the self-assessment is determined by three factors:
  - 1. Critical service scope
    - *Ask: Which service will be the focus of the self-assessment?*
  - 2. Organizational scope
    - *Ask: Which parts of the organization deliver the critical service?*
  - 3. Asset scope
    - *Ask: Which assets (people, technology, information, and facilities) are required for delivery of the service*

# Critical Service Scoping

- The CRR has a service-oriented approach,
  - one of the foundational principles of the CRR is that an organization deploys its assets (people, information, technology, and facilities) to support specific operational missions (or services).
- The CRR uses an identified critical service to frame the questions in the CRR.
  - must select a critical service in your organization that will serve as the focus of the assessment.
- A critical service is defined as follows:
  - *A set of activities that the organization carries out in the production of a product or while providing services to its customers, that are so important to the success of the organization that disruption to the service would severely impact the organization's operations or business.*

## Examples of Critical Services in an Organization

- some examples of organizations and their typical critical services that might be selected as part of a CRR:
  - banks and other financial institutions: clearing and settlement, mortgage application processing
  - emergency services providers: processing 911 calls, dispatch
  - electrical power plants: electricity generation, electricity distribution
  - hospitals: clinical services, prescription management
  - government agencies: court case management, benefit management
  - manufacturing companies: machining operations, order processing
  - airports: air traffic control, fuel management

## Organization Scoping

- Organizational scoping considerations can be gathered by asking the following questions:
  - *What part(s) of the organization is responsible for the delivery of the critical service?*
  - *Who are the owners of the assets required for delivery of the critical service?*
  - *Who is responsible for the critical service?*
  - *Who are the key stakeholders?*
  - *What asset types are used in the delivery of the service?*
  - *What risks have been identified for the service?*
  - *Who are the custodians of the assets used in the delivery of the critical service?*

So obviously it would be different set of people there may be some intersection there and then You normally do this in a workshop mode, so you bring everybody together and you actually do a workshop day long workshop, so you have to tell what are the terms and terminology that you use, what are the services that you are going to put in the assessment like not necessarily all services may be assessed, what are the what is the organizational environment context, what are the implemented practices, when do you say a practice is implemented, when do you say it is not and then response scale like yes, no or partial and then some follow on activities, what you will do after the assessment is completed, you generate the report then what are you going to do after that.

Table 2: Key Roles in the Self-Assessment Process

| Role | Description and Responsibilities |
|---|---|
| sponsor | The sponsor should have a broad understanding of the importance and components of the service for which the self-assessment is being completed. General responsibilities include<br>• deciding whether the organization should conduct a CRR Self-Assessment<br>• selecting an individual to serve as the facilitator<br>• ensuring that the resources necessary for the self-assessment are available<br>• communicating the organization's support for the self-assessment |
| facilitator | The facilitator is identified and assigned by the sponsor to have overall responsibility for preparing the organization for and conducting the CRR Self-Assessment. General responsibilities include<br>• completing the three phases of a self-assessment process<br>• working with the organization to ensure the self-assessment produces high-quality results<br>• facilitating the completion of the self-assessment form<br>• generating the CRR Self-Assessment report<br>• distributing the CRR Self-Assessment report to the sponsor and designees<br>• assisting in the planning of follow-on activities |
| subject matter experts (SMEs) | During the self-assessment, SMEs provide answers that best represent the organization's current cybersecurity capabilities in relation to the function being evaluated. It is most helpful for a SME to be<br>• closely involved in the planning, implementation, or management of the domain represented<br>• able to represent organizational functions being assessed<br>• able to represent one or more of the organization's activities in the CRR's 10 domains |

# Identifying Participants

Table 3: Identifying Participants

| Domain/Expertise/Function | Name(s) of SME/Participant |
|---|---|
| Asset Management | |
| Controls Management | |
| Configuration and Change Management | |
| Vulnerability Management | |
| Incident Management | |
| Service Continuity Management | |
| Risk Management | |
| External Dependencies Management | |
| Training and Awareness | |
| Situational Awareness | |

So then you know we went through this interpreting the self-assessment report, so you know some basic rules of we already went through this and we already discussed that if you get all the.. So we are in the report that I showed you is MIL 0.

# Topics to Discuss at the Start of the workshop

Table 4: Topics for Discussion at the Start of the Workshop

| Topic | Discussion |
|---|---|
| Organization's vocabulary | Discussion of terms found in the CRR that may prompt discussions relating to terms used within an organization. |
| Agreed-upon service and scope | It is important to remind the participants that the self-assessment is being applied to a specific set of activities performed by the organization and to describe those activities prior to beginning the workshop. |
| Organization's environment | It is useful to discuss the organization's environment to add context to the description of the service being evaluated. |
| Implemented practices | When completing the self-assessment, participants must consider practices as they are implemented on the day of the workshop. Do not consider activities that are planned or are in the process of implementation. Likewise, do not consider practices that have not been performed for extended periods of time. For example, if the organization has a disaster recovery plan that, in the opinion of the participants, is out of date to the point of being unusable, the plan should not be considered. |
| Three-point response scale | Participants use a three-point response scale to evaluate the degree to which the organization has implemented each practice. Review with the participants the meaning of each of the three response options so that all participants have a common understanding of when a particular response will be used. |
| Follow-on activities | It is important to discuss how the self-assessment will be used within the organization's overall cybersecurity program. The facilitator should emphasize that next steps will be based on the organization's risks and maturity. The facilitator should also point out the roles of participants in follow-on activities. |

# Interpreting the CRR Self-Assessment Reports

- CRR Scoring
- The scores for practice performance determine the scores for goal performance, which in turn determine the final scoring result for each domain, expressed in the MIL scale.
- Scores of MIL0 and MIL1 indicate base practice performance.
- Scores of MIL2 through MIL5 indicate institutionalization of practices.
- Basic Rules
- 1. Practices are either performed (answer = "Yes"), incompletely performed (answer = "Incomplete"), or not performed (answer = "No").
- 2. A goal is achieved only if all practices are performed.
- 3. A domain is achieved at MIL1 if all the goals in the domain are achieved.
- 4. A domain can be achieved at higher levels if the MIL questions for each level (MIL2 through MIL5) are answered "Yes."

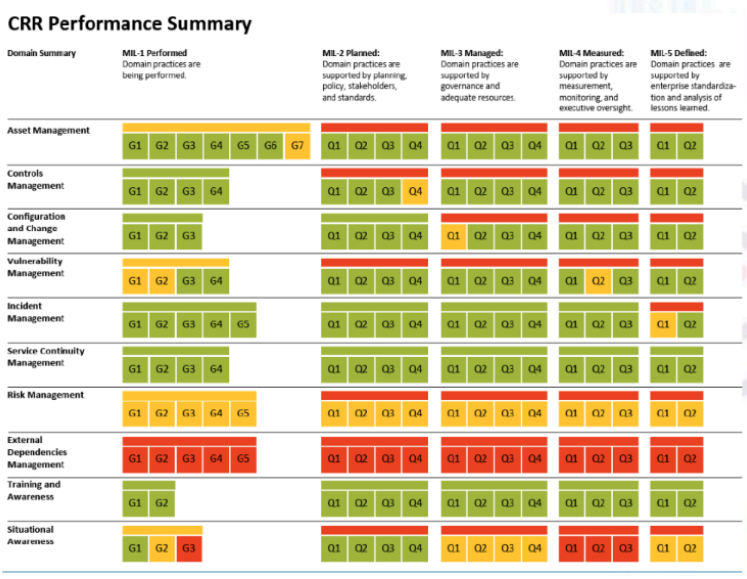
# Scoring Rubric

- Step 1: Score the Practice Performances per Domain
- Each practice in a domain is scored as follows:
- • *performed* when the question is answered with a “Yes” (green)
- • *not performed* when a question is answered with an “Incomplete” (yellow) or “No” (red) or “Not Answered” (grey)
- • if “Not Answered” (grey) is shown, the question was left blank and is scored the same as a “No”

- Step 2: Score the Goal Achievement per Domain
- Each goal within the domain is then scored as the following:
- • *achieved* when all practices are performed (green)
- • *partially achieved* when some practices are performed (yellow)
- • *not achieved* when no practices are performed (red)

# MIL Level Determination

- Step 3: Score the Maturity Indicator Level per Domain
- Each domain is assigned a MIL based on the following:
- • MIL0 if only some of the goals are achieved
- • MIL1 if all of the goals are achieved
- • MIL2 if MIL1 is achieved and all of the MIL2 questions are answered Yes
- • MIL3 if MIL2 is achieved and all of the MIL3 questions are answered Yes
- MIL4 if MIL3 is achieved and all of the MIL4 questions are answered Yes
- • MIL5 if MIL4 is achieved and all of the MIL5 questions are answered Yes
- MILs are not the same as capability levels, which can be assigned only after a formal appraisal of capability maturity, not after using an assessment-based instrument.




So some goals are achieved. MIL 1 is that all goals are achieved. So we did not get any of the area in the report that I showed. There was not a single domain at MIL 1. Unless you are in MIL 1, you cannot be MIL 2.

MIL 2 requires additional questions and so on so forth. So we discussed this. And this is how the performance summary looks like we already looked at this. So, that is it. So, we will stop here for the resilience review part of the course and now we will move on to next class we will move on to the threat intelligence sharing with STIX. So, that is where I think that is more or less where we will be next week we may do some evening classes additional evening classes to finish this curriculum. Thank you.