Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 03
Lecture: 08

Now, as I said in the beginning, there are three different approaches to GRC - Governance, Risk and Compliance, GRC. One approach is to follow frameworks like the COSO, COSO ERM or COBIT, which are fairly large and very detailed frameworks, I would say for large organizations. If you have a startup in IIT Madras Research Park, you do not have to think of COSO ERM. So you are a small organization or even if your organization is a mid sized organization, the ERM may not be the approach. But if you are, say into e-commerce or your business is online business and your customers actually reach you through the online mode and if you are not concerned about security, then there is an issue. You may not have to worry about a large enterprise framework for risk management.

Your governing body may already be doing it. They may be aware of it, but they may not have invested in big standards or audits of that kind, because those are all investments. But cyber security definitely is something that you need to manage because of the assets. And so sometimes for technology organizations, the major category of assets is the cyber assets.

And therefore, think of in my MIS course, I asked students to compare Madras Cements versus Infosys, compare the assets. It is not the equipment, manufacturing equipment that form the assets of IT or a technology organization. It is basically the cyber assets including people. And therefore, it is different in terms of the strategy to protect them or safeguard the assets. So that is where the standards that are specific to cyber assets become important.

Standards which are specific to cyber assets. And that is what the ISO / IEC standards are about. So these are standards developed specifically for cyber security management, very specifically for cyber security management. It began with the ISO 1700 standards or sorry, it is not ISO 1700, BS 7799. It began with BS 7799 meaning it is a British Standard, which was developed for cyber security management.

And ISO adopted this and it became an ISO standard later. So I will show you different variants or different types of ISO standards specifically for cyber security management. So BS standard is the fundamental standard where the ISO standard originated for cyber

security. And ISO / IEC 17799 : 2005 has 133 possible controls. So it is like a large standard and it was renamed as ISO 27000 series starting with ISO 27001 which is the basic standard in the PDCA format.

Have you heard of PDCA ? If you worked in industry, particularly manufacturing industry, which I did. PDCA is a common term. Plan Do Check Act. Plan Do Check Act. We saw a similar set of processes for COBIT But essentially plan before you do, plan and do, then check whether what you did is correct and then act on it.

So PDCA is very intuitive. So you do for especially, for activities for process improvement in manufacturing and in of course, whenever you have technology, you need to improve continually and PDCA is such a framework. So it followed, ISO 27001 basically is a standard to ensure that your cyber security systems are active and is in the improvement cycle. So you have today, what in the industry or in the standards body there is a set of standards known as ISO 27000 series of standards. ISO 27000, whenever you hear keep in mind that it refers to cyber security management standards provided by ISO.

And if you go to the ISO website , you will see that these standards run into several, more than 50 and each of them addresses a very specific cyber security management requirement. For example, infrastructure management, there are separate ISO 27000 series for infrastructure. So which standard you need to implement ? It could be, if you talk to ISO consultants they would say no, not just one, you need this, you need that, they will try to sell as many standards as possible. You know that we are an ISO certified organization, IIT administration not academics. So as an example, I want to show you the 46th standard of ISO 27000 series.

ISO 27799 is a standard information security management in health, using ISO / IEC 27002 guides. So the fundamental standard is a 27002 but it has been customized or it has been specified particularly for certain horizontals and verticals I would say. Healthcare is a vertical where there is a specific ISO 9000 standard. Infrastructure management is a horizontal but it may have a specific standard. So they have developed specific standards for various verticals and horizontals of IT.

This is one way to abstract it, what is ISO? What does ISO standards do? They have different standards that you can adopt depending on the nature of use of IT and the nature of your business. If your healthcare is your business then they will offer one and if within healthcare depending on the nature of IT application, they will actually offer a set of standards. So for example there is a standard for network security. So it actually works in, across different dimensions as I said, vertical and horizontal. Now you need to

appreciate that the standards are developed by certain bodies and there is politics also.

So as managers you should not be very naive, you should also know well what is going on because consulting organizations would approach you as managers, well, why do not you go for ISO. And keep in mind that all of these are investments and you need them but there is competition as well in the industry for standards. So as I showed to you there are GRC approach, there is ISO approach and then you will also see, there is a competing body known as NIST. So ISO standards have been criticized, if you actually read literature and in particular ISO is not something that is very acceptable in the United States. Although today's US organizations also go for ISO but their preferred cyber security standard would be the NIST.

Because it is developed in the United States, particularly for US military and such kind of sensitive applications of cyber or IT. ISO is European and well, that actually informs you about what politics you can accept in terms of interest. So each regions and regional politics will have its own interest. So there are criticisms, I am not making a very informed statement on politics because some of those allegations may be correct as well but I am only providing you what is available in the public domain, in terms of claims and criticisms of different standards. So NIST, I think it is expanded as National Institute of Standards and Technology.

This is actually a US standard setting body not just for cyber security but for generally for technology. So if you have to understand say about cloud computing technology standards etc. you can again go to NIST and look at that. So it is a generally standard setting body for technology. So NIST has worked intensely and intensely on cyber security and developed several standards.

But a distinction of NIST standards is that unlike ISO, they are accessible, accessible openly. These are open standards. We call them open standards. These are not proprietary standards. If you have to get an ISO 27001 series of standards and even for understanding how is the documentation done, what are the different courses of different standards, in 27001 series.

It is not available in a open domain. If you search for it you do not get it. But if you want to access NIST SP 812 - computer security handbook, go and download it. It is openly available.

NIST standards are open. ISO standards are not. You have to pay for it. But one is to have the standards available open for developing understanding. But implementing a standard, may require more knowledge. So you have open source software and

proprietary software.

And all the world should be implementing open source solutions because they are free and they are open. But that is not what you see in the world. There is Microsoft. There is Oracle. And all these technology companies which sell software and make their money, they used to make their money through selling standard, sorry selling licenses so far.

Of course, the mode is changing to cloud. But in any case, they make their money out of the software that they build. But at the same time you also see similar software, database. There are open source databases.

But the world is a mix of both. If you look at in terms of adoption I would say, the proprietary software are used more than the open source software. Why so? Here again the debate between ISO and NIST is open versus proprietary. So the whole world should be NIST while ISO is still prevailing. Just think and respond, give one or two possible reasons. Maybe Sir, at times the open source is also not entirely free.

If something like premium, some version, the initial version that is free and the upgrade version that is costly. That is true in the case of software I agree. There is a basic version like you know, you may be working with R, R studio, for example. The basic version is free but if you have to develop applications using R, studio etc.

Then you have to pay premium. So this one way of attracting people onto that platform. In platform based business basically you need participants, you need people to start using it. So that is another approach basically to sell something at the end. But there are software which there is no interest to sell anything at all. It is for consumption by a community without commercial interest, that also exists.

So your first answer is that support. Something is available free but who will implement this and who will continue to support us when it is implemented? So that is a important question. So the service part. Product is available but service. So and essentially today's scholars would argue that it is service that you consume.

It is not the product. Product is basically to provide you certain services. So the service fulfillment is the most important thing. Not buying the product. So therefore that is a missing element and if a proprietor like Microsoft sells, its operating system, it comes with both.

So therefore that is a challenge. The second is reputation. I think you are referring to reputation. So having a standard like ISO which has certain reputation in the market

versus having something which does not have equal reputation. Well, is NIST reputed? Yes, it is reputed. But it is only a standard in an abstract form but implementation requires expertise or specific expertise and knowledge.

And there, of course you may need consultants. Is there anyone in the class who have worked on NIST standard? Anyone from industry? No. ISO, ISO 27001. Depends on the class size when I teach executives, of course they come out openly with what they did and what their experiences are.

So that is fine. It depends on how much of practice you are familiar with. This is perfectly fine. So, there are guides and standard specifications by NIST which you can access and then get more familiar with. So soon I will be giving you an assignment.

Do not worry. That will help you familiarize with NIST. And NIST's website is something that all students should visit to get a sense of what these standards are. And then in order to work on one assignment, you will require one or more NIST standards. For example, how do you do contingency planning systematically? So there is NIST standard available for that.

So you do not have to imagine many things. You do not have to develop this aspects from the scratch. This is already specified. Of course, you have to think through your problem or your context and customize it but you have to have a broad framework available for different activities pertaining to cyber security management. So, are there any questions at the end? So the purpose was to familiarize you with the frameworks and standards for cyber security at a practice level or at the industry level. If you have comments and questions, you can put it straight away or else we would actually discuss a case for the day.

So let us have the first case discussion by the student groups. So the first group is going to discuss the case of iPremier. So iPremier is a case that is shared with you and iPremier has three versions A, B and C. Today we are going to discuss the first, A.

Sounds like a detective story. So let us actually get into the details. And this is a case I think, how our business school documented in the 2000s. When I started teaching MIS, I came across this case and they have updated it around here, you can see there is a 2018 version of it, which is what we are going to discuss in the class. Alright friends, please come over and take charge. Next 30 minutes is yours.