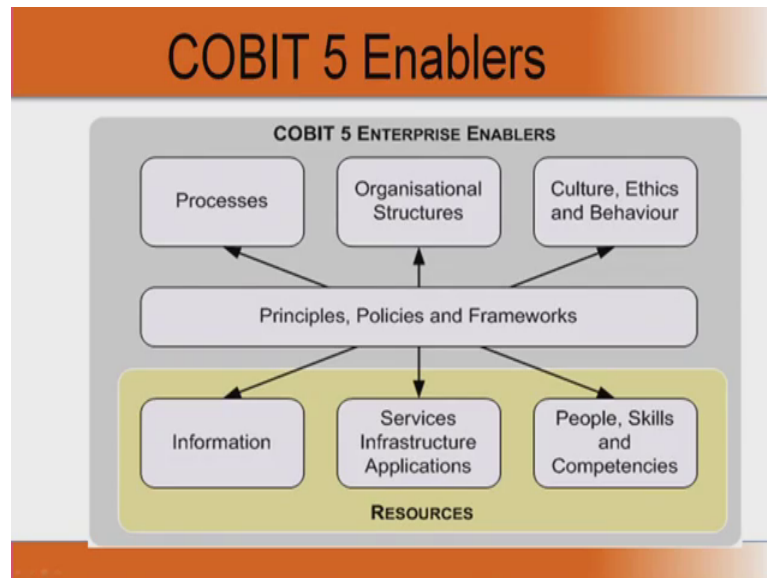


Introduction to Information Security
Prof. Dilip H. Ayyar
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 30

(Refer Time Slide: 00:34)



What are the COBIT 5 enablers, now if you see the core, it is the principles, the policies and the frameworks through which lot of things are connected like your processes, the organizational structures, the culture, ethics, and behavior, and then the resources. In resources, you have information as a resource services, infrastructure applications are resources people skills, and competence are resources.

Now, the bottom half under resources, if you remember a couple of slides back, we discussed that effectiveness, efficiency, confidentiality, integrity, availability, reliability, and compliance are required. It required for 5 aspects, which are they: technologies facilities people, data, and application. So, the bottom half, the one where the resources are mentioned, are for those 5 aspects information is a resource infrastructure, that is technology, applications, facility, that is your infrastructure, it will cover there, people, and data is information, or data is information is derived from data. So, a people is also covered people, skills, competence.

(Refer Time Slide: 01:48)



Governance and Management

- **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions and options; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and progress against agreed direction and objectives (**EDM**)
- **Management plans, builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (**PBRM**)

So, these are the enablers for COBIT 5. Now let us look at governance and management, what is governance ensure it, ensure the your enterprise objectives are achieved by evaluating the needs of stake holder, the conditions for ensuring that governance, and the options for setting directions, or guiding the organization through prioritization and decision making.

So, basically COBIT will help you to, convey what does the stake holders, needs are what are the conditions under which, your objective should be met, and what are the options, what directions need to be said for decision making are for prioritizing, what has to be done, what, when, why. So, the governance will ensure that, the important thing is monitoring the performance, the compliance, and progress, against the agreed direction, and objectives, that is EDM, agreed direction, and objective.

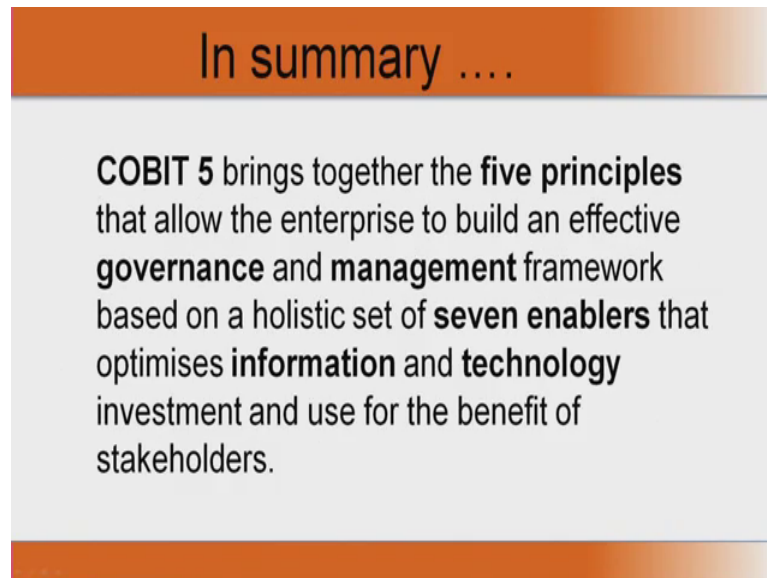
Now, monitoring is a very crucial aspects, it is not enough to just implement, or to formulates some policies, or say that this is, what have to do, and then forget about it, you need to monitor, whether the processes, or working as intended. Whether people are following the processes, as laid down, and whether complaints to regulatory fiduciary, what are being achieve, whether progress is being made.

So, all these things you need to monitor on a constant basis. So, governance will help you to, achieve all this, it also helps in management plans bills, new runs, or runs monitors activities in alignment with the directions, set by the governance body to achieve your organizational, or enterprise objectives. Again management will plan they

will build means, whether it is infrastructure, or the direction.

Whatever, it is said, it runs that particular plan, and then it monitors, whatever is being laid down, to ensure that you know the governance body, you can monitor, whether all the organizational objectives, are being met.

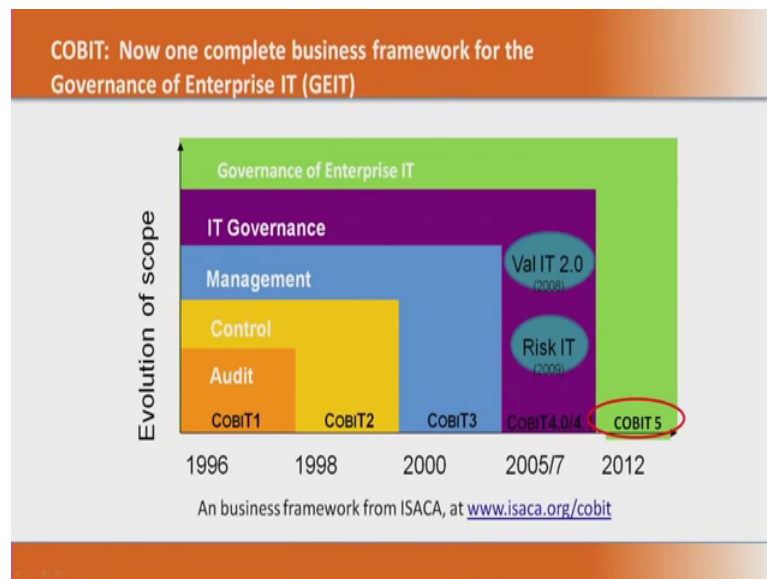
(Refer Time Slide: 04:21)



So, in summary, what does COBIT do it, brings together in the 5 principles, we have seen what are the five principles, which allow the organization, or enterprise to build an effective governance, and management framework, based on what it is based on holistic, set of 7 enablers that, optimizes IT, investment, and use and benefit of the stack holders.

So, in simple terms, what does COBIT to it, ensures or it gives your direction, for achieving what it needs to achieve, what is that is to be achieve effectiveness, efficiency, confidentiality, integrity, availability, complaints and reliability. For what are those are the 7 enablers right. for what 5 principles application, technologies, facilities, people and data.

(Refer Time Slide: 05:20)



Now, let us look at COBIT from where, it started in 1996, it addressed the audit aspect in COBIT 2, the controls are improved, you can see that is the evaluation of scope. So, it basically started as a audit objective, expanded to controls, further expanded in COBIT 3, 2 covering the management aspects, further expanded to IT governance. So, you can see the shuttle difference in each of the versions, and then finally, in 2012 COBIT 5 covered all of these, that is governance of enterprise IT.

So, governance of enterprise, IT included all of the 4 things, which is audit, which is control, management, governance, all put together, you get governance of enterprise IT. You can read more about COBIT, what it does, what the standard tells you at ISACA.org/COBIT. Now, we have seen what COBIT is, but how is it implemented, so the improvement of governance of enterprise IT.

(Refer Time Slide: 06:43)

COBIT 5 Implementation

- The improvement of the governance of enterprise IT (GEIT) is widely recognised by top management as an essential part of enterprise governance.
- Information and the pervasiveness of information technology are increasingly part of every aspect of business and public life.
- The need to drive more value from IT investments and manage an increasing array of IT-related risk has never been greater.
- Increasing regulation and legislation over business use of information is also driving heightened awareness of the importance of a well-governed and managed IT environment.

So, governance of enterprise IT is called GEIT, there is also a certification by ISACA, which is CEGEIT, which is widely recognized by top management, as it is an essential part of enterprise governance, so corporate governance of enterprise, at our governance of enterprise IT, is viewed by the top management as a very important aspect of enterprise governance information, and pervasiveness of information technology, are increasingly a part of every aspect of business and public life, which is the case now, and the need to drive more value from IT investments, so you need to leverage IT, to perform better way organization, and managing a increasingly, increasing array of IT related risk, which was never been great . So, as your networks are your corporate IT becomes more complex then, IT related risks also increase.

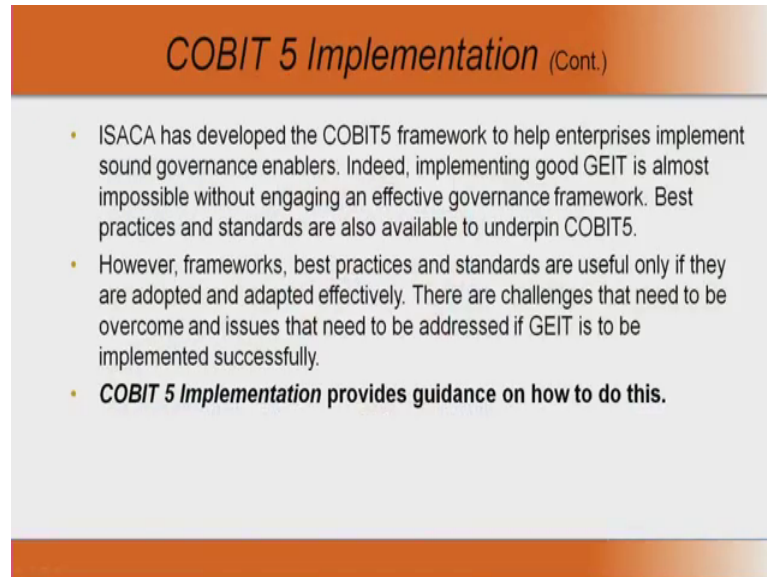
So, you need to drive value from IT, by exploiting the technology at the same time minimizing the risks, that the technology brings you with. You need to provide increasing regulation and legislation, over business use of information. So, that is also leading to a heightened awareness, and importance of using a well governed IT environment framework, for managing the IT environment.

So, again you have compliance loss, you have regulatory requirements fiduciary requirements, you have legislations over business use of information. You take an example, can you actually govern a data center, which is hosted in Russia, but the actual uses in India. So, which logs are applicable for the data, which is residing in Russia, but which is used in India, that is example of this.

So, you need to have more control, over your IT legislation, IT in use of information. So, you need to have a proper governance mechanism, to manage at IT environment, you

need to address all those factors, when your managing the IT environment. So, COBIT 5 helps you in that.

(Refer Time Slide: 09:21)



COBIT 5 Implementation (Cont.)

- ISACA has developed the COBIT5 framework to help enterprises implement sound governance enablers. Indeed, implementing good GEIT is almost impossible without engaging an effective governance framework. Best practices and standards are also available to underpin COBIT5.
- However, frameworks, best practices and standards are useful only if they are adopted and adapted effectively. There are challenges that need to be overcome and issues that need to be addressed if GEIT is to be implemented successfully.
- **COBIT 5 Implementation provides guidance on how to do this.**

Now, ISACA has developed this COBIT 5 framework, for what purpose that is to help the enterprises implement, sound governance enablers. So, implementing good, GEIT is almost impossible, without engaging an effective governance framework. So, best practices and standards are also available, to under pin COBIT 5. Frameworks, best practices standards are useful only, if their adopted and adapted effectively.

So, it is not just a copy and paste. You need to adopt the standard, to suit your IT requirement, and you need to implemented properly. So, that you get maximum leverage, maximum benefit out of the implementation. There are challenges that need to be overcome, and issues that need to be addresses addressed if GEIT is to be implement implemented successfully.

So, having just frameworks, and best practices, and policies and standards are useful only, if they are effectively implemented, followed, monitored. Otherwise, your GEIT is not going to be successful, what COBIT 5 does that, implementation will help you or guidance on how to do this, because it will be an iterative process, where you can tune and fine tune the implementation, and bring it to an optimized level

(Refer Time Slide: 10:47)

COBIT 5 Implementation (Cont.)

- COBIT 5 Implementation covers the following subjects:
 - Positioning GEIT within an enterprise
 - Taking the first steps towards improving GEIT
 - Implementation challenges and success factors
 - Enabling GEIT- related organisational and behavioural change
 - Implementing continual improvement that includes change enablement and programme management
 - Using COBIT 5 and its components

What as it cover, the COBIT 5 implementation, it covers positioning of governance of enterprise IT within an organization, and it takes a first step towards improving GEIT, implementation challenges, and success factors. It will teach you these are the challenges, that have faced when I have tried to, implement the corporate enterprise governance in corporate enterprise IT, and this is what needs to be done, to fine tune the process.

You enable governance of enterprise IT or related organizational, and behavioral change. So, for any changes something, that people in an organization, do not want to do. Take for example, an organization in a manufacturing sector, or in pharmaceutical sector have been using a certain software, for a certain period of time. Suddenly the management decides that, they want to improve the governance they need to have better control over IT.

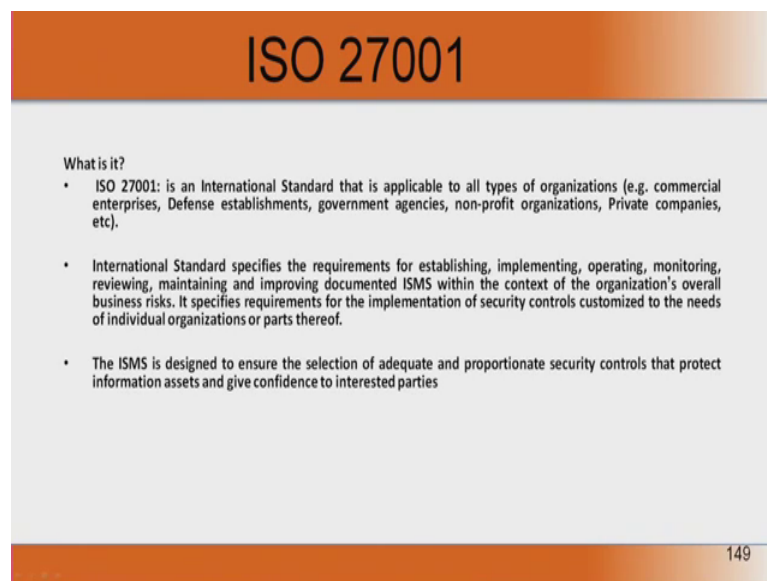
So, they decide to introduce SAP, now the first reaction from the users, would be wide the system needs to be changed, everything is working fine. We are very comfortable with that, so the needs to be a process, to educate on the benefits. So, it is done through a chain process, which is you go to unfreeze the users, from the existing environment. You have to move them, to the new environment gradually, and then you have to refreeze them in the new environment.

So, basically you have telling them, you will have to educate them the benefit, of using the new system. In this case, the SAP, tell them why the old system needs to be replaced, explain to them, the governance of enterprise IT, what benefits it could bring for the organization, and to the users as employees of the organization. What benefits they are

going to achieve it, may be reduction in the process itself, then implementing the continual improvement, that includes change enablement and program management.

So, it also helps in your continual improvement, because it is an iterating process, it is just like the quality process, where we do a plan do check and act. So, this your monitor and evaluate, and then optimize all those things what we learned in a few slides ago, will be repeated or iterated over and over again, until you get an achievement or a complaints achievement, or a satisfactory level of optimization. We will see what is COBIT 5 and it is components.

(Refer Time Slide: 13:58)



The slide features a title 'ISO 27001' in a large, bold, black font at the top center. Below the title, the text 'What is it?' is followed by three bullet points. The first bullet point states that ISO 27001 is an international standard applicable to various organizations. The second bullet point describes the standard's requirements for ISMS. The third bullet point notes the standard's goal of ensuring adequate security controls. The slide number '149' is located in the bottom right corner.

ISO 27001

What is it?

- ISO 27001: is an International Standard that is applicable to all types of organizations (e.g. commercial enterprises, Defense establishments, government agencies, non-profit organizations, Private companies, etc).
- International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.
- The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties

149

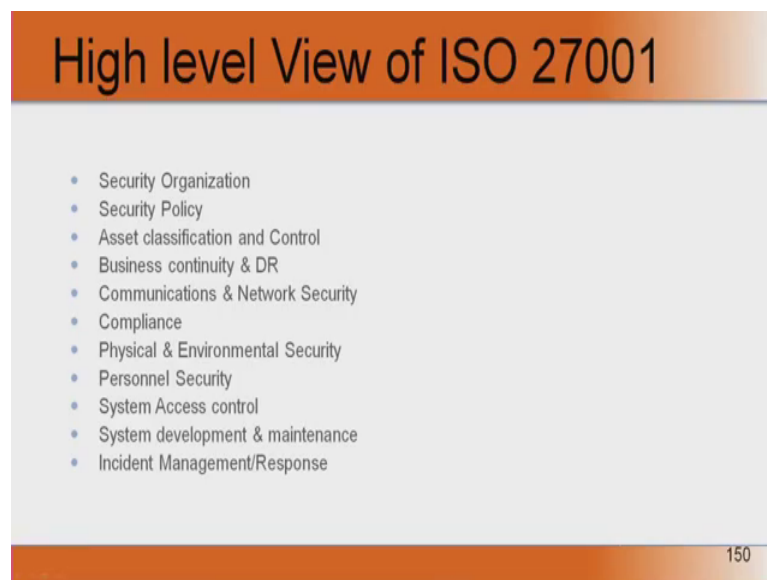
Let us talk about 27001, ISO 27001. 27001 is also a standard for a information security. Now, the latest version is 27001:2013, the year at which it was released, but what is 27001. It is an international standard, that is applicable to all types of organizations; commercial enterprises, defense in an there are instances, where in UK in the early stages of 27001, or company with no computers have got certified for 27001, that means that was a 2 member organization, with no computers on board.

But they still got certified for information security standards. So, 27001 cover all types of organization, the predecessor to 27001 was 17799, and the predecessor to that was BS, British standard 7799. Now, once it became an international standard, it became 27001, there has been 2 or 3 revisions, since, these standard was implemented. 27001 is an international standard, which specifies or requirement for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving documented information

security management system, ISMS, within the context of organization's, overall business risks, now the entire dictionary, English dictionary is there in this, establishing, implementing, operating, monitoring, reviewing, maintaining, and improving documented ISMS. It specifies, the requirements for the implementation of security, controls, customized to the needs of individual an organizations or parts of that. There may be organization, where certain clauses of 27001 are not applicable.

So, they need not be implemented, there may be clauses, where you know entire bunch of section may not be applicable. So, they may not need to implement it. So the ISMS is design to ensure that, the selection of adequate, and proportionate security controls, that protects the information assets, and give confidence to the interested parties. So, by implementing this ISMS, it gives as a sense of assurance, to the interested parties to the stake holders of the organization, to the customers of the organization, to the users of the organization, that appropriate are adequate controls, have been built in to, which will help the organization achieve IT governance. Again go back to COBIT, to have a effective control, over enterprise governance of IT, and 27001 is, the only information securities standards, that covered most of the aspects of a IT environment.

(Refer Time Slide: 17:23)



Now, what is the high level view of a 27001, when you read the standard, it is pretty difficult to understand, what exactly is going on in that. There is several controls 100 plus, 133 control. Then these are the objective and all that, but to simplify it, you look at the slide, I will just explain to you need to have a security organization, meaning you need to have a proper, forum at the top of the organization, which will give direction to

the information security function, within the organization.

Now, in the security organization you can nominate a CISO, chief information security officer; under him, you can have information security officers; under them You can have information security auditors, or at the same line that is FOR auditing. So, once your organization is set in its place, then what would you do, you need have a security policy. What is a policy, we have discussed in domain 1. Now the policy in simple terms is a statement or intent from a top management on what needs to be achieved or what needs to be followed, within the organization are not, it is very simple, when you go out of your house, you lock the door. Why do you lock it, so that the thief does not come in, similarly in an organization a policy is made, to say what you can, and what you cannot do within the organization. Now, locking a house is an undocumented policy it is practice.

So, there are several things in information security, which the organization may be doing as a practice, but not actually written down as a policy. In ISO 27001, you write it down as a policy, and follow it. So, that gives directions to the organization, to follow a better control over information security. So, now, after you have written the policy, you classify the asset now, asset again we come back people, process and technology or assets.

So, you take as asset you take a server, that is an asset. You classify based on what based on, its criticality to the organization. What would happen, if the particular asset is lost, data is lost, if there is a theft of that asset, if there is a crash in the network, or communication line, or the hard disk, what would happen, what are the consequences for of that, what are the controls you need to put into prevent all these things.

Somebody from physically damaging the server, from copying data from the server., so all those things need to be specify, then you specify what are the controlled requirements, what kind of protection I need for this asset, how much protection is needed for this asset. It again depends on the criticality, of that asset, and then you have the business continuity, and disaster recovery plan in the event of a natural disaster, or due to a human error or errors in the process or failures of a component failure of the server itself, or the failure of a network equipment, or the communication lines. What would happen to the business, how much what are contingency plans, you have in case that the business or the IT fails, whether you need to operate out of a different site, that is hot site, warm site, cold site, reciprocal agreement. We will discuss all these in the forth coming domains, but here to emphasize BCP and ARP addresses, all those things the continuance plan the

business, impact analysis, your disaster recovery plans, everything is addressed, then this BCP and ARP.

Then the communication and network security, what kind of communication links I need 2 ISDN lines, 2 lease lines. I need of fail over the for one lines. So, I need to have a load balance around my communication, so, that my service to the clients, or service to the internal employees are not affected, what kind of security do I put in for the network, I need to put in a firewall, I need to put in a intrusion prevents in system, I need to put in a unified, threat management antivirus.

So, that comes under communication, and network security, then the compliance with the regulatory bodies. If it is bank, it is RBI, if it is insurance it is IRDS. So, whatever I do within the frame work of IT, should comply with the loss or regulations said by the government, or the regulatory bodies. Then you are physical and in environmental security adequate measures should be there, your server should be housed in a very secure room with different levels of access control, in big data center, they may have biometric, they may have proximity cards, or they may have a simple lock and key for a small organization, but then the underlying fact is that, you are physically protecting your server, and network equipment. Environmental security that is protection, against your smoke detectors, smoke, fire extinguishers. All those things, you put into place properly monitoring, and controlling the temperature within your data center, or server room.

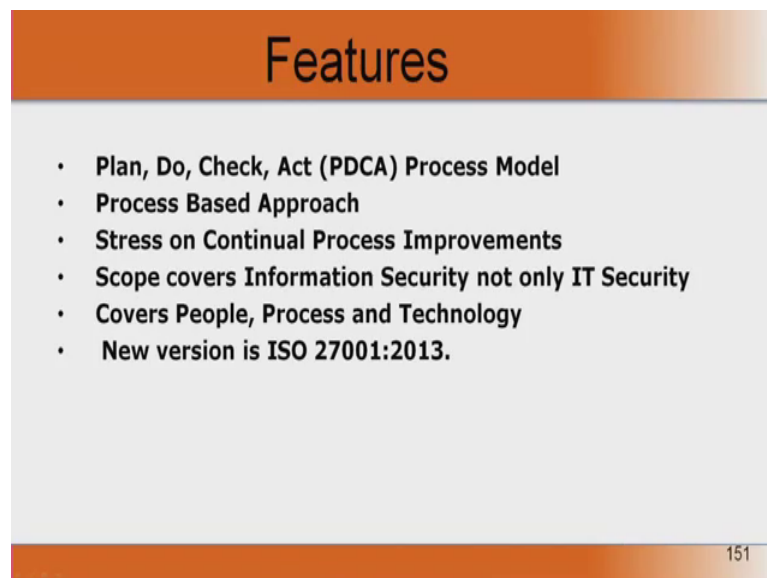
All those will be covered under environmental security. In physical also ingress of external vendors coming in, whether proper procedure are followed by your security guards, to allow entries to only authorized personnell, after due verification from the concerns. All those things will be covered. Then the personnel security, that is the security of employees, which is perhaps the most important, out of all these, because you have to ensure that, all employees are safe and they are taken care of as the first measure, when it is comes to an organizational security. System access control, what are the methods and ways in which a person can access as a system, what kinds of control are you putting into, for a person, to log into a network. Whether, it is through a simple log in id or password, or through a 2 factor of authentication or array, or whatever technology biometrics, those are defined in system access control.

These also depend, upon the organizations requirement, it is not necessary or it is not laid

down that, you should have this for do getting access to the system. You need to have a minimum set of guidelines, and standard that is to be followed for ensuring this. Then, if it is an organization with system development, then this clause is applicable system development, and maintenance. What are the methods under which, a system can be develop, what are the minimum set of requirements, that have to be specified for information security, whether a proper system development life cycle methodology has been followed. How the system is maintained, whether proper change control is there, proper versioning system is there. All those things are addressed in system development, and maintenance and then incident management, and response. incident, what happens in the event of an incident.

So, something undesirable happening in an organization is an incident. So, what happens if an incident occurs, how do you manage that incident, what are the processes in which, you need to respond to the incident, as and when it occurs. The incident can be a simple human error, and server weakness, and natural disaster any of the kind, but you need to address, and document and be prepared on how to react when an incident occurs.

(Refer Time Slide: 26:10)



Features

- **Plan, Do, Check, Act (PDCA) Process Model**
- **Process Based Approach**
- **Stress on Continual Process Improvements**
- **Scope covers Information Security not only IT Security**
- **Covers People, Process and Technology**
- **New version is ISO 27001:2013.**

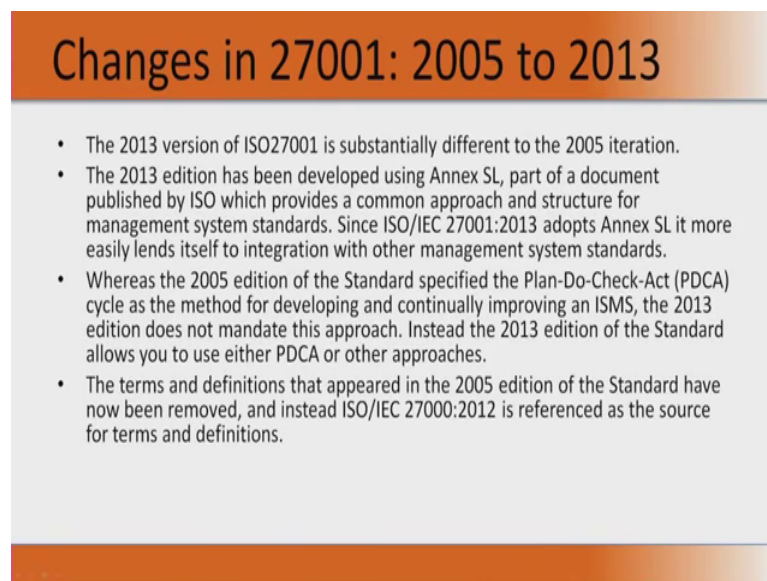
151

What are the main features of 27001. Upto 27001:2005, PDCA was a process model, that was used. Now, PDCA was developed plan, do, check and act, it is a quality process, which was develop by Dr Edward William Deming. And that was the model, which was followed in ISO, 27001. In 27001:2013, it has significantly changed. Now, the process that was followed in up to 2005, it was process based approach, that is it was the following the PDCA model. And \tThe stress was on continual process improvement.

And the scope covers information security not only IT security. So, what does it mean, IT security is any security that is related to the information technology, whereas information security is you cover the entire organization, where ever information is generated, stored, altered, destroyed, in all those places you need to apply. So, the scope covers not only your iIT process, but your non IT process also. Physical access is not in IT process.

But it is a process, which impact organizations. It covers people, process and technologies. So, we have spoke about that, it covers all the aspects, which is people, process and technology, and the latest version is, version 27001:2013

(Refer Time Slide: 28:00)



Changes in 27001: 2005 to 2013

- The 2013 version of ISO27001 is substantially different to the 2005 iteration.
- The 2013 edition has been developed using Annex SL, part of a document published by ISO which provides a common approach and structure for management system standards. Since ISO/IEC 27001:2013 adopts Annex SL it more easily lends itself to integration with other management system standards.
- Whereas the 2005 edition of the Standard specified the Plan-Do-Check-Act (PDCA) cycle as the method for developing and continually improving an ISMS, the 2013 edition does not mandate this approach. Instead the 2013 edition of the Standard allows you to use either PDCA or other approaches.
- The terms and definitions that appeared in the 2005 edition of the Standard have now been removed, and instead ISO/IEC 27000:2012 is referenced as the source for terms and definitions.

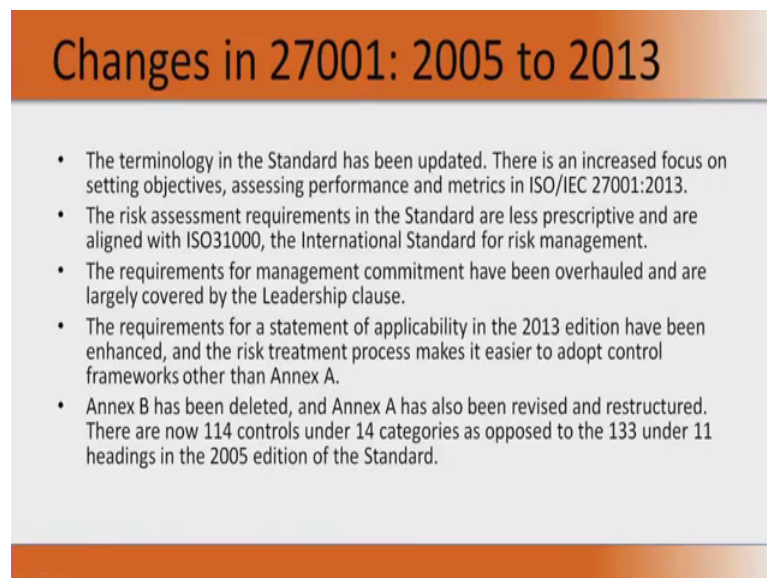
Now, there are changes in 27001 from 2005 and 2013. So, we have seen the 11 domains of 27001 starting from security organization, to incidents response or incidents management. In 2013, the standard itself has been altered substantially, to suit the current requirements. It was, it has been developed using the annexure, SL, part of the document, published by ISO, which provides the common approach, and structure for management system standards.

Now, this particular annexure, this was developed using the annexure SL. So, 2013 adopts the annexure SL for implementing 27001. But in 2005, this standards specified the PDCA cycle as them method for developing, and continual continually improving a ISMS. But in 2013, the edition does not mandate the approach that means, it is an optional thing, but 27001, 2013 of the standards, allow you to use either PDCA or other approaches also.

Now, you can use ISO 31000 as an approach for managing your risks, but you can have that in conjunction with PDCA. So, the standard now does not specify that, you have to use this model alone. You can use any model, that you deem fit for your organization, and the terms and definitions that had come in 2005 edition have now been removed. So, there was at glossary of terms and definitions, that were there in the 2005 edition.

Now, 27000, 2012 is referenced as the source for the term and definitions. So, it has been realigned drastically, to meet the ever increasing demands in IT , and also to optimize, so again the 27001:2005 to 2013 has seen a maturity, how it as to be implemented. The terminology in the standards have also been updated, there were certain definition given for certain terminologies, which has been updated again to meet the current scenario.

(Refer Time Slide: 30:23)



Changes in 27001: 2005 to 2013

- The terminology in the Standard has been updated. There is an increased focus on setting objectives, assessing performance and metrics in ISO/IEC 27001:2013.
- The risk assessment requirements in the Standard are less prescriptive and are aligned with ISO31000, the International Standard for risk management.
- The requirements for management commitment have been overhauled and are largely covered by the Leadership clause.
- The requirements for a statement of applicability in the 2013 edition have been enhanced, and the risk treatment process makes it easier to adopt control frameworks other than Annex A.
- Annex B has been deleted, and Annex A has also been revised and restructured. There are now 114 controls under 14 categories as opposed to the 133 under 11 headings in the 2005 edition of the Standard.

And now there is an increased focus on setting objectives, accessing the performance, and metrics in at 2013 edition. The risk assessment requirement in the standard, is less prescriptive, and are aligned with ISO 31000, so again 27001 as we said in the first slide is a information risk management under or international standard for risk management.

So, here the standards have been aligned, with 31000. So, that you get an effective, and much optimized level of risk assessment, there is management. The requirement for management commitment, have also been overall. Management commitment, was in fact one very important aspect of 27001:2005 which again overall and now it is covered by leadership clause.

So, anybody having a leadership role in this implementation is what is covered now,

rather than the management commitment. So, earlier they would say that, you need show management commitment, when you write how do you check management commitment. There security policy has been written, we see whether it is been approved by the board of directors of the organization.

It has to mandated be approved by the board of the directors also, but then they can delegate to certain leadership. So, that has been slightly altered, and requirement for statement for applicability, have been enhanced, and the risk treatment process, makes it easier to adopt control framework other than annexure A. So, there was specification annexure A, that should have use this particular model, now that has been enhanced; annexure B, there was annexure B in 2005 version which has been deleted.

Annexure A, also has been revised, and restructured. Earlier there were 133 controls under 11 headings or 11 domains. Now, there are 114 under 14 categories, you can read about what is 27001:2005. It is a very good reference point, to understand what information securities. Then later go on to 2013. So, that you will understand the differences, between 2005 and 2013 editions and also will give you a better...