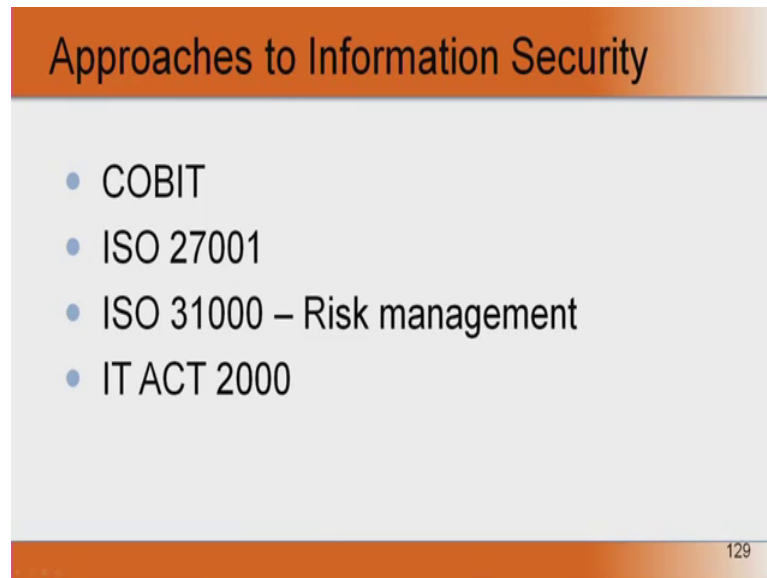


**Introduction to Information Security**  
**Prof. Dilip H. Ayyar**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Madras**

**Lecture – 29**

(Refer Time Slide: 00:11)



The slide features a title bar with a gradient from orange to white, containing the text "Approaches to Information Security". Below the title bar is a light gray rectangular area containing a bulleted list of four items. The bottom of the slide has a solid orange bar with the number "129" in white text on the right side.

- COBIT
- ISO 27001
- ISO 31000 – Risk management
- IT ACT 2000

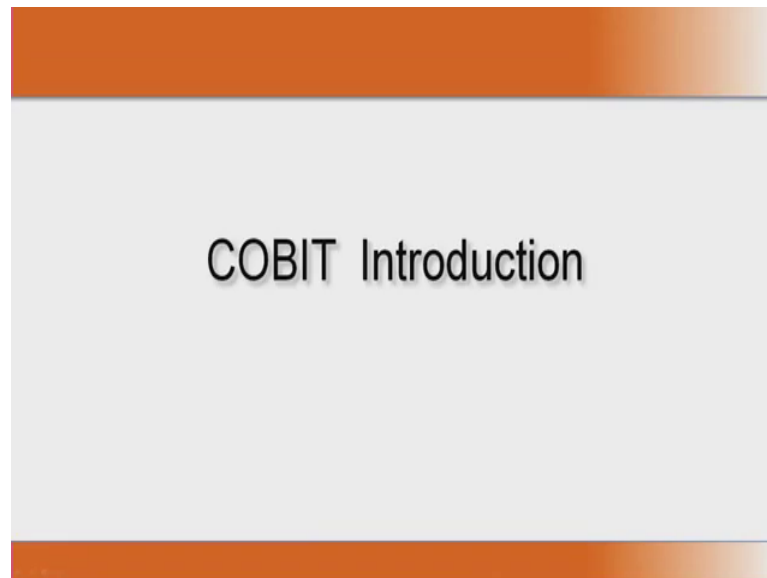
The last part of module 2, I will be covering. We will take a look at, what are the approaches to information security, why do you need different approaches. Now, risks affecting organizations can have consequences in terms of economic performance, and professional reputation, as well as other factors such as environmental safety and special out comes, societal out comes.

So, managing risks effectively helps organizations to perform well in an environment full of uncertainty. So, that is why need different approaches to information security. There are different standards available for information security one is COBIT, which we will discuss in detail, ISO 27001 which is for organization security, and ISO 31000 for risk management.

So, 31000 is becoming more popular, it is basically principles and guidelines, it provides principles, framework and the process, for managing risk. It can be used by any organization regardless of the size, or what activity it performs are even, it is not depended on the setup. Using 31000 also can help organizations increase the likely hood of achieving their objectives,

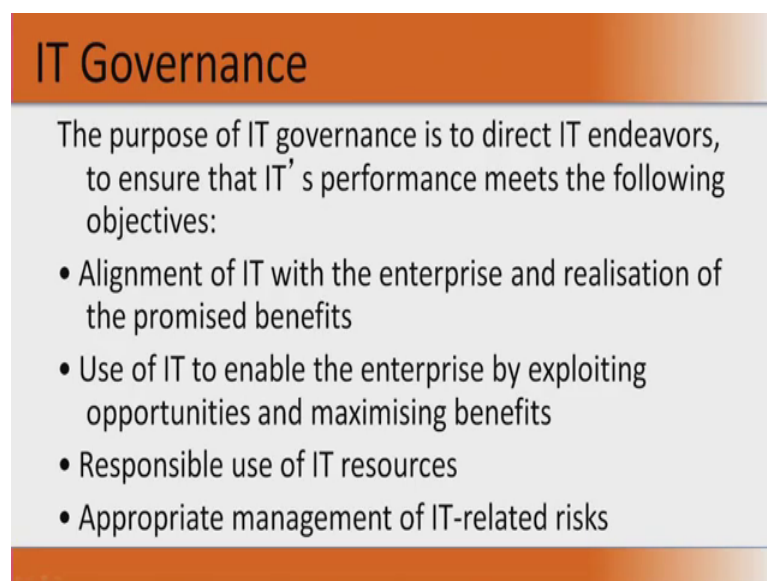
improve the identification of opportunities, and threads effectively, allocate used resources for risk treatment. Then we will look at IT act 2000, some of the important clauses of IT act an 2000, not all of them in detail.

(Refer Time Slide: 02:03)



Let us see, what COBIT is first of all, what is the purpose of IT governance, the purpose of IT governance is to direct the IT endeavors, ensure that IT's performance meets this is a certain objectives.

(Refer Time Slide: 02:06)



What are the objectives, alignment of IT with the enterprise and realization of the promise benefit, so what does that mean, your business objective should be aligned, or

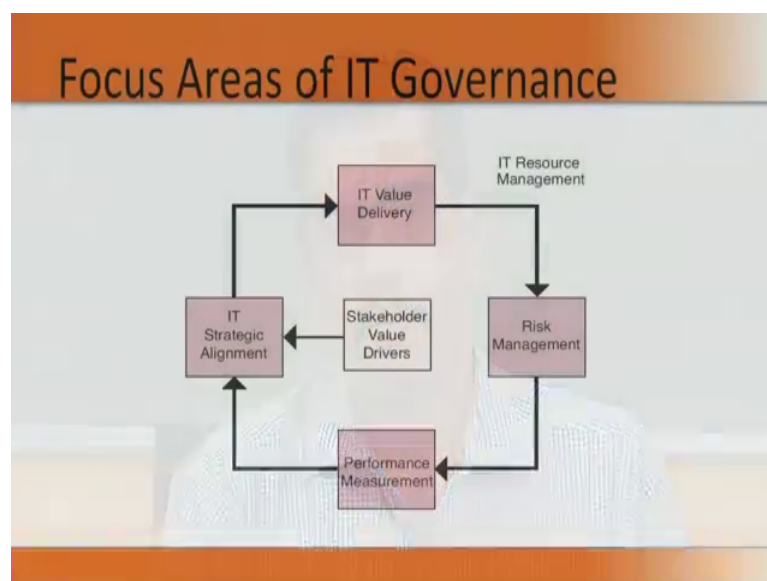
you should have a clear business objective, your IT objective should align with the business objective. So, that you can achieve, what do you want to achieve as an organization, and simplify and optimize the processes. When use of IT, to enable the enterprise by exploiting opportunities, and maximizing benefit.

So, again you use IT to the optimum by exploiting opportunity. So, what are the exploited opportunity that you to may want to exploit, one is you want to do a data analysis of your market it, you are competitors market competitors, to see how better you can project a product of services, and in what kind of resources you will use to achieve that. May be you may optimize, it to bring a reduced work force.

So, you use it to enable the enterprise by exploiting opportunities, and maximizing benefits. Then responsible use of IT resources, use IT resources for doing the something beneficial to the organization, to achieve it is goals, rather than just left right and center implementing IT. Then appropriate management of IT related risk, what does this mean.

So, you need to have a risk based approach, and manage it efficiently to see that most of your measures are most of your measures mitigate the risk, that comes out of your IT infrastructure. Now, what are the focus areas of IT governance, you see the slide there is stakeholder value driver. So, there is something which is a value or there is a vision for the stakeholders.

(Refer Time Slide: 04:28)

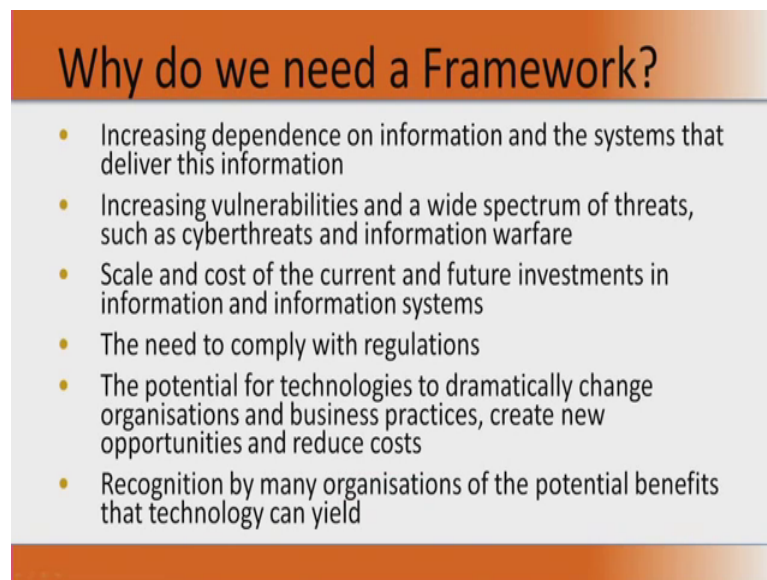


The IT strategic alignment should be there with the vision, that is on your left hand side of the white box. There should be, from these strategic alignment, there should be a value

in the IT delivery. Similarly, IT resource management should be optimized, which in turn, should lead to your risk management process. Then, you measure the performance.

And so this is basically a cycle, where the IT governance revolves around these areas, one is your strategic alignment of IT with your stakeholder values, or your business vision. Then you have the actual delivery of IT values. Then, you have the resource management, which is the people management technology, management process management. Then, your risk management comes into the picture, where you effectively identify the controls or the risks. Then you measure the performance, for enhancement this cycle continuous.

(Refer Time Slide: 05:51)



### Why do we need a Framework?

- Increasing dependence on information and the systems that deliver this information
- Increasing vulnerabilities and a wide spectrum of threats, such as cyberthreats and information warfare
- Scale and cost of the current and future investments in information and information systems
- The need to comply with regulations
- The potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs
- Recognition by many organisations of the potential benefits that technology can yield

Now, why do you need a framework, is the question, increasing dependence on information and the systems that deliver this information. So, you have everything on the system today, on our large network, large database. So, you depend on the information that the system gives you, or you derive information, or you make business decision based on what, the system is giving you.

So, you need a framework to protect the IT resources, and infrastructure increasing vulnerabilities, and a wide spectrum of threats, such as cyber threads and information warfare. We will look at cyber threats information, warfare in domain 3 which deals extensively with your kinds of threats, that is virus and malware, information warfare.

So, since vulnerabilities also are increasing on a day to day basis and more and more new threats are coming in.

You need a framework, to safeguard your information and information resources. Then your scale, and cost of the current and future investment in information, and information system. Organization generally spend, or organizations generally spend a lot of amount of money, and make investment for the future for the information, and information systems. So, you need a framework to actually follow the practices. Then, the important thing is you need to comply with regulations, there will be regulatory bodies.

If it is bank, you have reserve bank, if you have insurance if you have an insurance company you have an IRDA. So, if you have a stock, a broken company, then you have BSC NSC. So, you need to comply with the guidelines released by these regulators from time to time. So, you need a proper framework to address your risks. Then the potential for technologies to dramatically change organizations, and business practices create opportunities, and reduce cost.

So, as we discussed earlier the technology itself has a immense potential to dramatically reorient the organization by introducing business practices, by creating new opportunities. Example, data analytics or you do analysis are market competitor analysis, to find out what best way you can do to, sell your products or services. Then, recognition by many organizations, of the potential benefits which the technology can yield now, lot of organizations today realized that, without technology there is no way forward.

(Refer Time Slide: 09:02)



Successful organizations understand and manage the risks associated with implementing new technologies.  
Firms need to ensure that -

- IT provides value - Cost, time and functionality are as expected
- IT does not provide surprises - Risks are mitigated
- IT pushes the envelope - New opportunities and innovations for process, product and services

So, you need to implement IT in a very responsible way, and ensure that the organization follows some framework, for better business, for better security, and better management of information, and information resource. And, if you see the successful organization also understand, and manage the risk associated with implementing new technologies. So, organizations need to ensure that, IT should provide value it that means, at the cost the time and functionality, are as expected in simple term you implement it.

It should give you the information, that you require at that time you require, at the same time it should not be at a very high cost, and it should give you the desired functionality. You should not be able to get the result, which you require in a roundabout way. It should be a straight forward, simple mechanism. IT does not provide surprises, risks are mitigated.

So, by implementing IT once, you mitigate risks you address the vulnerabilities, the threats, the risks. It does not provide surprises it means, it works as intended. So, you design it to work, in a particular way it will work in that particular way provided your risks are mitigated

IT pushes the envelope new opportunities and innovations for processes products, and services. Again with the implementation of IT, you have new opportunities for innovation and it for creating a new process, for creating a new product, or to deliver a new service.

(Refer Time Slide: 10:37)



## Who Needs a Framework?

- Board and Executive
  - To ensure management follows and implements the strategic direction for IT
- Management
  - To make IT investment decisions
  - To balance risk and control investment
  - To benchmark existing and future IT environment
- Users
  - To obtain assurance on security and control of products and services they acquire internally or externally
- Auditors
  - To substantiate opinions to management on internal controls
  - To advise on what minimum controls are necessary

But who needs of frameworks. Now, if you take the organizational hierarchy, the board and executive, why do they need to ensure that the management follows and implements the strategic direction of for IT management. So, the board and executive will basically say that your management down below, follow a set of rules, follow a set of framework and implements the direction for IT.

So, basically they direct they are the ones, who say these are the policies that my organization needs, to follow and this is how we implement it. And this is what we need to do to take the organization forward that is as far as the board, and executives comes then the management can be in some places. They say, it is a senior management in some places, say it is a top management.

So, basically management is the top, the one's that are below the board and executive. Now, why do they need are they framework to make it investment decision for every small computer purchase, you cannot go to the board of directors, they may be having a limit beyond 5 lakhs or 10 lakhs. It needs to be approved by the board. So, till that amount, the management, the top management or senior management might take the decision.

So, if a framework is there, it will help the management to make better decisions. It will also help the management, to balance risk and control the investments. So, if a proper framework is there, the risk and we balance using proper risks assessment or risk mitigation or risk management methodologies and then control the investment. So, there will not be an unnecessary expenditure over IT, to benchmark existing, and future IT environment.

So, once you have a framework, let us say your organization follows COBIT, we are going to discuss later. So, COBIT once it becomes a benchmark irrespective of who comes, and goes COBIT as long as organization is that, that particular standard will be followed. Because you have already put in the framework people, already people are following it. So, it becomes a benchmark for existing, and future IT environment.

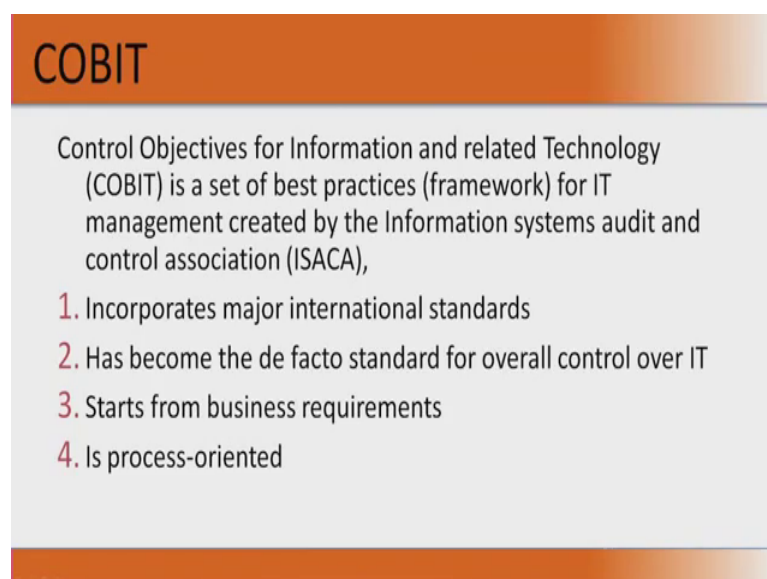
So, anything that you do with IT, you will say let us make it complain to COBIT, or let us make it complain to 27001, then the normal users, why they need a framework-to obtain assurances on security. And control of products, and services they acquire internally or externally. So, now the users need assurance in what way, that the product is safe or the software, then the use this safe and control of the services also they are

delivering is safe, and secure is irrespective of whether they obtain it internally or externally. So, they need an assurance, they need assurance which the framework can give because proper set of policies, a proper set of procedure are followed in the users, will get an assurance that the security and there is a control of products and services. The auditors finally, why to substantiate opinions to management, or internal controls, now it is very easy for an auditor, if he needs to audit an organization, say based on COBIT. I have seen lot of audits based on, we need COBIT complaints for SAP infrastructure, we need an ISO 27,001 certification, we need certification based on ISO 9126, or an audit based on framework of ISO, 9126.

So, from the auditors prospective, it is relatively easier to follow a framework and do the audit conduct an audit, and find out the results whether it is positive or not. So, that he can substantiate his opinions, to the management on what the internal control processors are existing in the organization. That will also give the auditor, a better understanding of what, to advice or what are the minimal set of controls, which are necessary for that organization, to improve on the information security infrastructure.

Now, let us get into what COBIT is, COBIT is control objectives for information and related technology. It is also a set of best practices are again, you can call it a framework for IT management created by the information systems, audit and controls association isaca. So, the entire COBIT slides that we are going to explain is made or rather owned by isaca, you would have heard of lot of certifications of isaca like in cisa, cism, crisc, cgeit. So, it is a same organization that is bought out COBIT.

(Refer Time Slide: 16:23)



**COBIT**

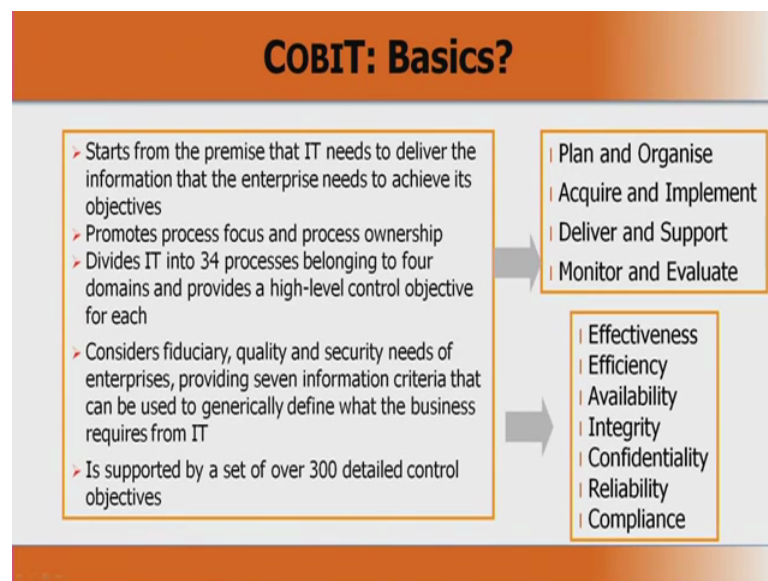
Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for IT management created by the Information systems audit and control association (ISACA),

1. Incorporates major international standards
2. Has become the de facto standard for overall control over IT
3. Starts from business requirements
4. Is process-oriented



COBIT actually incorporates major international standards. There are references to Cadbury, coco in COBIT. It has become a de-facto standard for overall control of IT. Again the moment you say that, you want to go for a COBIT certification, you know that the organization knows that, depth of COBIT. And what it needs to achieve COBIT complains, it starts from business requirements, and is process oriented. Now, when you say start from business requirement, itt is first you should know what your business requirement is, then you should know what your IT requirement is then you decide on what other controls you need. So, generally when you look at standards, they say this is your requirement in IT, this is what you need to do, and this is how you have to implement. Whereas, in COBIT they start right from the business requirement onwards, which is to ensure that your IT related requirements match with your or go in sink, with your business requirement. And it is process oriented in the sense for everything, there is a process and you need to follow the process, to achieve something. What are the basics of COBIT, it starts from the premise that, the IT needs to deliver the information.

(Refer Time Slide: 07:48)



That the enterprise needs to achieve objectives, that is it is telling that your IT, and business strategy should be aligned. It promotes process focus, and process ownerships. Let us focus on the process, that is followed and every process should have a owner, like you have seen in domain one there should be owner, custodian and user of information. Now, the process ownership is one particular process.

Let us say that, the management of a server is a process. Now, how who owns that process, who is the custodian of the process, who is the user of that process, what rights

that the people have in that, what they can do, what they cannot do, what happens if something goes also, all of these is the written down in a process. And the focus is on the processes and the ownership of that process. COBIT divides it into 34 processes belong in to 4 domains.

If you see on the right hand side plan and organize is one domain acquire an implement is another deliver, and support is a third one, and monitory and evaluate is the fourth one. So, it divides it into 34 processes belonging to these 4 domains. It considers fiduciary quality, and security needs of the enterprise, providing seven information criteria that can be use to define, what the business requirement from IT is.

So, basically if you see on the right hand side, there are 7 controls, 7 I'ss in all of the words on the right hand side, starting from the effectiveness to compliance, there are I's in every letter, the letter I. So, you see effectiveness, efficiency, confidentiality, integrity availability, reliability and compliance. It considers the fiduciary quality, and security needs of the enterprise providing seven information criteria.

So, these are the information criteria it is applicable to what, it is applicable to application technology facilities, people and data. So, this 7 for that I, so basically you need to remember, the 12 characteristics which is effectiveness, efficiency, confidentiality, integrity, availability, your compliance and reliability for applications technologies, facilities people and data. And it is supported by COBIT, is supported by a set of over 300 detail control objectives.

(Refer Time Slide: 00:34)

**Enterprise Benefits**

Enterprises and their executives strive to:

- Maintain quality information to support business decisions.
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.
- Achieve operational excellence through reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimise the cost of IT services and technology.

**How can these benefits be realised to create enterprise stakeholder value?**

What are the enterprise benefits of COBIT, now enterprises and their executives strive to or they try to maintain quality information, to support business decisions. So, that means, the information that is generated out of their IT system, should be of quality is fitness for use fitness, for purpose that is the definition of quality, but in this case it also means quality requirement can be, if it needs to be confidential, it has to be kept confidential data, should not be altered, that means it should maintain the integrity, and it should be available to authorized users at whatever time they require it. So, you need to maintain the quality of information to support business decisions. To generate business value from IT enabled investment that is to achieve strategic goals and realize business benefits through effective and innovative use of IT.

So, now the organization as spend a lot of investment, or made a lot of investment in IT, so they need to not only achieve their goal, and realize the benefit for their business, but they also need to generate business from that. It is not enough that, you have some IT systems in place, and you are doing something. But you need to derive value, out of your IT system. So, that your organization performs more optimally, and you generate more business out of that framework, that you follow.


Can you achieve operational excellence, through reliable and efficient application of technology, now what is operational excellence, that is the operation, should be stream length you go from step 1, 2, 3, 4, 5, but through IT if you are able to go from step 1, 4 and 5, that is optimization of your processes. So, basically you are trying to be more efficient in your operational practices, and you try to emulate excellence through reliable and efficient application of IT.

You also maintain IT related risk at an acceptable level. So, there is nothing called zero risk, you need to have risk at an acceptable level, there may be cases where you cannot even handle that risk, or put some controls for certain kind of risk. So, you transfer the risk through insurance, or it may be because your technology used is old. So, you need to replace the technology, or repair the technology.

So, that is another thing, or even retire the technology. So, may if you have a server take an example that, you have a node server, you cannot do many, and you cannot install new software's in that. So, you need to either upgrade the server to perform, to what you require it is you try to repair or try to replace that. Even then you cannot try to retire that itself, that I do not want these server, let me look at some other alternate form of doing it.

Then, you optimize the cost of IT, and IT service and technology. Now, how can these benefits be realized, to create enterprise stockholder value. We will look at that, what is stakeholder value, stakeholder, stockholder I mean different people use different thing for the purpose of COBIT, let us use, stakeholder value.

(Refer Time Slide: 20:40)



## Stakeholder Value

- Delivering enterprise stakeholder value requires good **governance and management** of information and technology (IT) assets.
- Enterprise boards, executives and management have to **embrace IT** like any other significant part of the business.
- External **legal, regulatory and contractual compliance** requirements related to enterprise use of information and technology are increasing, threatening value if breached.
- **COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.**

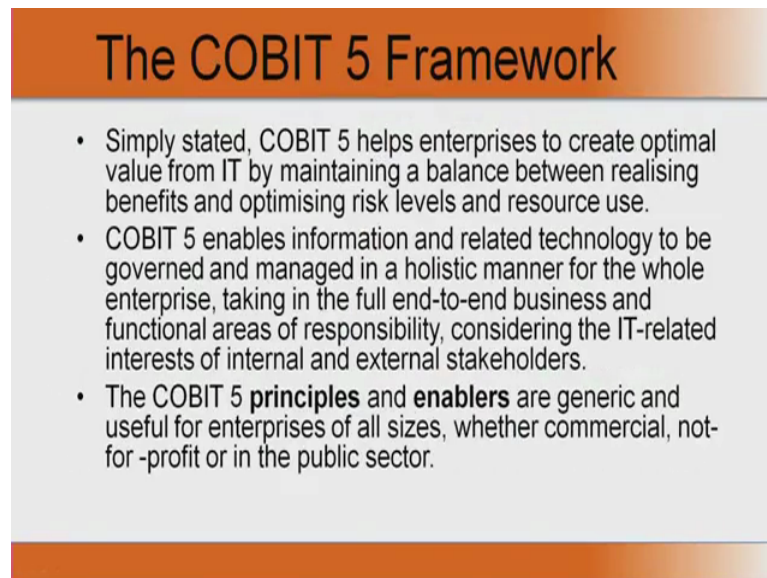
Now, delivering enterprise stakeholder value requires good governance and management of IT assets. Now, we have seen what an asset is, so if you need to what are the assets, let us say in simple terms, people, process and technology are assets in an organization. So, almost everything is covered in people, process, and technology. Now, you deliver enterprise stakeholder value, to deliver that you need to have a good governance of IT, and then you boards your executives, the managements all have to embrace IT, like any other significant part of the business. You should not use IT as a method, or as a mode of just doing some business, you should leverage to the maximum extent. So, that your board of directors of the organization, the executives and management should treat it, and use it like any other significant part of business, like your sales or marketing function which actually brings in business. So, you need to leverage IT also to that level.

Your external legal regularity, and contractual complains requirements related to enterprise use of information, and technologies are increasing, threatening value, if breached. External legal regularity complaints requirements again, they require a lot of controls, and place lot of framework in place and the penalty for not complying and the obligations of not complying, the fines of not complying are too high so, you need to have a proper framework in place of the stock stakeholder, should realize that having an

effective framework is going to help the organization. You have discussed about all these things, and COBIT 5 provides these things, what does It provide a comprehensive framework, that assists the enterprises to achieve their goal, and deliver value through effective governance, and management of enterprises.

Last 2, 3 slides we have seen, why of framework as require, who requires of framework, and what the stakeholder value is in implementing of framework. All this put together, is available in COBIT 5, because it provides a very comprehensive framework that the enterprises need or require to achieve their goals, and values through effective governance. That is you govern effectively, and manage the IT enterprise, or the it unit effectively, so that you can leverage, maximum benefit out of it.

(Refer Time Slide: 27:43)



The slide features a title 'The COBIT 5 Framework' in white text on an orange gradient background. Below the title, three bullet points are listed in black text on a light gray background. The slide is framed by orange borders at the top and bottom.

## The COBIT 5 Framework

- Simply stated, COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.
- COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.
- The COBIT 5 **principles** and **enablers** are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

The COBIT 5 framework itself, let us take a look at it COBIT 5, or COBIT helps the enterprises to create optimal value for IT by maintaining a balance, between realizing the benefits and optimizing risk levels, and resources. So, again we are talking about optimization. So, you have to derive the maximum, from your IT infrastructure, but for doing that you should still maintain a balance between, realizing benefit, and optimizing risk level.

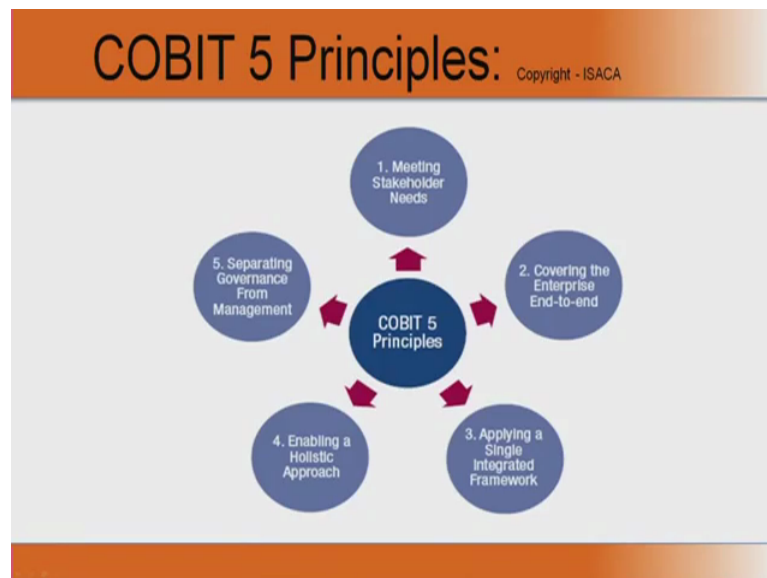
So, you should not do something, which will put your IT infrastructure at a risk, or the information are information resources at a risk. You it COBIT 5, actually helps view to create that balance, because of the processors it follows. COBIT 5 enables information and related technology to be governed, and managed in very holistic manner for the

whole enterprise, for the entire enterprise taking in the full end to end business and functional areas of responsibilities.

Considering the IT related interested for internal and external stakeholders. So, COBIT 5 also enables the governance, to be managed in a very holistic manner for the entire enterprise, taking in the full end to end buss, that is what we defectively means it addresses issues end to end. In the area of responsibility, again we have seen something called ownership, which was discussed earlier.

It not only addresses the issues for the interest of your internal stakeholders, but also the external stakeholders. The COBIT 5 principles and enablers us are generic, and useful for enterprises of all size, whether commercial, whether it is a not for profit, or if it is a public sectors. It does in matter, which is going to use COBIT 5. COBIT 5 is equally applicable to all.

(Refer Time Slide: 30:06)



Now, this image also has been taken from isaca. If you see at the center, look at the slide COBIT 5, the first is you need to meet the needs of the stakeholder. We have to discuss that, second is COBIT 5 cover the enterprises end to, that is from the business needs to the IT needs, you are applying a single integrated framework. Like we discussed earlier, it is a framework, which addresses or start from the business, and then goes to the IT requirement, or IT implementation. So, it covers the end to end enterprise, IT governance. So, you it is a single integrated framework, which covers both the business, and IT side it has a holistic.

