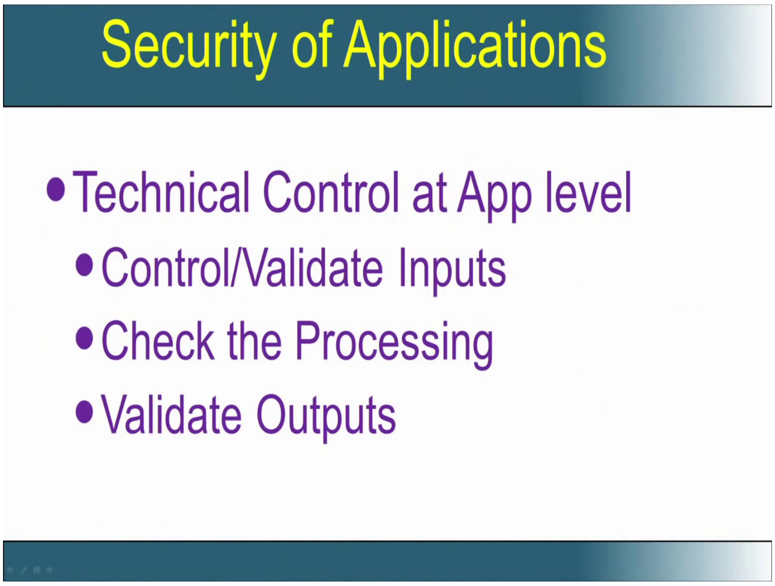
Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 13

Now, we will see controls that could be applied at an application level.

(Refer Slide Time: 00:16)



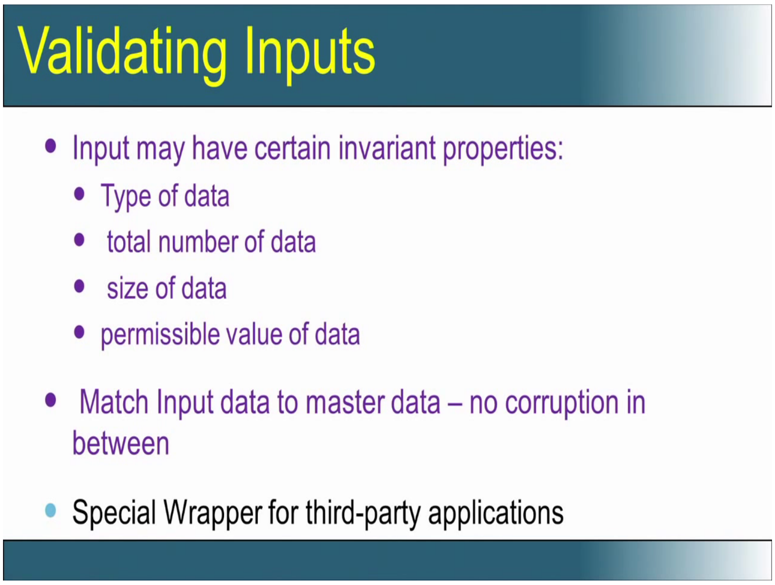
Security of Applications

- Technical Control at App level
  - Control/Validate Inputs
  - Check the Processing
  - Validate Outputs

We have seen that controls are very important to implement information security policies. We have seen controls for the people. We have talked about access control; we have talked about passwords, which are much more applicable to people. Now, we will see controls on processes and technology specifically the applications. What is an application? An application is a software; an application can also be a process; a policy, that is, a procedure that is followed by an organization.

Now, let us consider an application as a software. Now, what can we control on the software? This software can be purchased from commercially of the shelf from a… With a commercially of-the-shelf software, what you go and control? We can do three things; we can control the input; we can control the output; and, we can also instrument and control the processing. So, let us see what do we mean by controlling the input; what do you mean by controlling the processing; and, what do you mean by controlling the output.

(Refer Slide Time: 01:43)



Validating Inputs

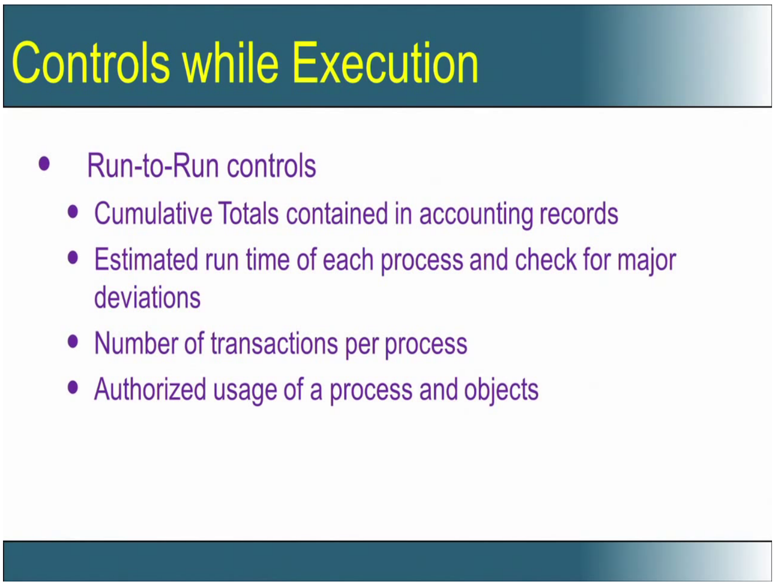
- Input may have certain invariant properties:
  - Type of data
  - total number of data
  - size of data
  - permissible value of data
- Match Input data to master data – no corruption in between
- Special Wrapper for third-party applications

Now, look at validating inputs. The control that you could have on an input is basically to go and check whether the input is proper. What do you mean by the word – proper? Inputs can have certain invariant properties. We can go and check whether those invariant properties are satisfied. For example, the type of data; the input should be an integer; we give say a floating point number; or, the total number of data; it takes 5 different fields as input. The size of data – it takes an array of 10 integers on a permissible value of data. The data should be in some range; it should not cross this range. For example, the data should be in the range between 1 and 3. So, when an input is given to a particular software, these inputs will have certain invariant properties and we can go and check these invariant properties for the consistency.

We can also match the input data to the master data. So, the input data, which is received by a module, you could have a check, go and query the database at least occasionally or on some sensitive operations to see what is there in the database is reflected. It is not corrupted by any intermediate applications before it reaches a particular application. And, we need to have… Suppose we have third party applications that we have purchased commercially of the shelf; then, an organization could actually write wrappers around these software to go and validate the inputs, so that when the inputs go into the system, we are very sure that the correct inputs go; and, something, which is not to be gone into the… – which is not to be input into the system.

For example, there could be a software for which we would have three modes of operation and we do not want to give a fourth mode. So, when the mode, which is an input to the application, is to be entered into the application, before it enters, you can have a check and say whether the value is in the range 1 to 3. A very very simple concept, but very difficult interface – implement especially in the case of very complex interfaces. But, validating an input can solve many problems. Down the line in the level 3 or level 4 course; where, we will talk about security of architectures. We will go and elaborate this on how do we build architectures, trusted architectures using untrusted components or components for which we will not be in a position to go and prove it is trustworthy. So, validating inputs will be dealt in much more detail in those phases of this information security course.

(Refer Slide Time: 04:57)



Controls while Execution

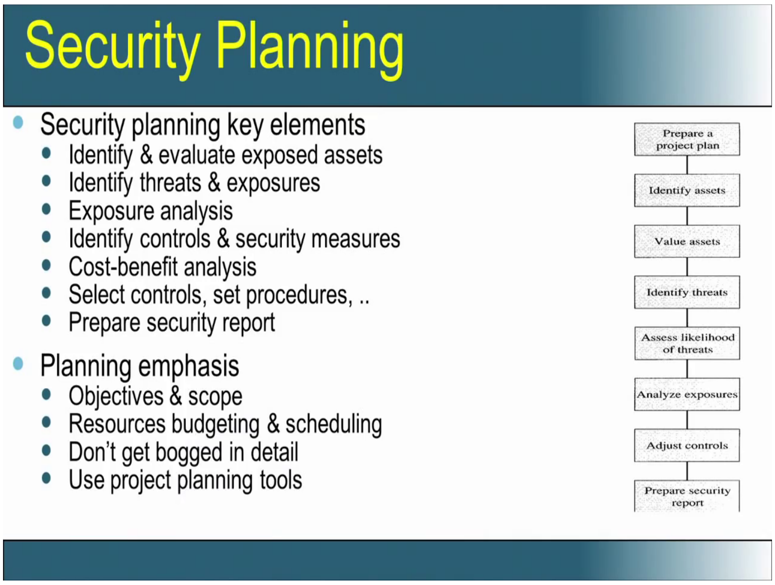
- Run-to-Run controls
  - Cumulative Totals contained in accounting records
  - Estimated run time of each process and check for major deviations
  - Number of transactions per process
  - Authorized usage of a process and objects

Now, the next thing as we discussed is to control while you are executing. What do you mean by control while we are executing? There is something called run-to-run controls. What do you mean by run to run? Let us again take a banking application. So, there is a transaction. So, from an account, for example, the total amount of transaction; so, suppose you are crediting into an account; the balance before the transaction plus the input that is given for the transaction, which is the amount to be credited, should be equal to the balance after the transaction. So, they are very very simple check. So, these type of checks needs to be evolved when somebody develops the application. If you are buying a third party application, you need to develop the wrappers or modules around that application to make these type of sanity checks. Another interesting check we can say; suppose a bank is giving a loan against a deposit. So, somebody puts say 5 lakhs and they are giving a loan; the loan amount should not be greater than the deposit amount. It is a very very simple rule. So, these types of checks are what we mean by these run to run controls.

These run to run controls can be a little more than this. For example, one can go and find the estimated run time of each process. While you are actually implementing the software, while you are doing a performance monitoring of the software, you can estimate for each transaction what some estimated time; you can estimated the time. And, if this time is going to be exceeded beyond some threshold; say suppose a process should take say 10 milliseconds; it is taking thousand milliseconds; it is taking 1 second; then, we would like to go and see what happened there. Another type of run-to-run control is that, for a particular function or a process, there would be say 10 transactions. If there are going to be 12 transactions, then there is something wrong. So, we can go and find the number of transactions that has happened on the database for a particular functionality and established a run-to-run control.

Last thing of course, which operating systems support in a large way, is authorized usage of a process and object. So, these procedures have to be executed only by users with this much amount of privilege. These objects can be manipulated by users with this amount of privilege. So, those things come into… If you start enforcing them, they are also run-to-run controls. So, though we may have an application, which is third party, for which we do not have the source code, a lot of things that we could do by understanding the environment in which this process is going to work.

(Refer Slide Time: 08:14)



Security Planning

- Security planning key elements
  - Identify & evaluate exposed assets
  - Identify threats & exposures
  - Exposure analysis
  - Identify controls & security measures
  - Cost-benefit analysis
  - Select controls, set procedures, ..
  - Prepare security report
- Planning emphasis
  - Objectives & scope
  - Resources budgeting & scheduling
  - Don't get bogged in detail
  - Use project planning tools

Prepare a project plan

Identify assets

Value assets

Identify threats

Assess likelihood of threats

Analyze exposures

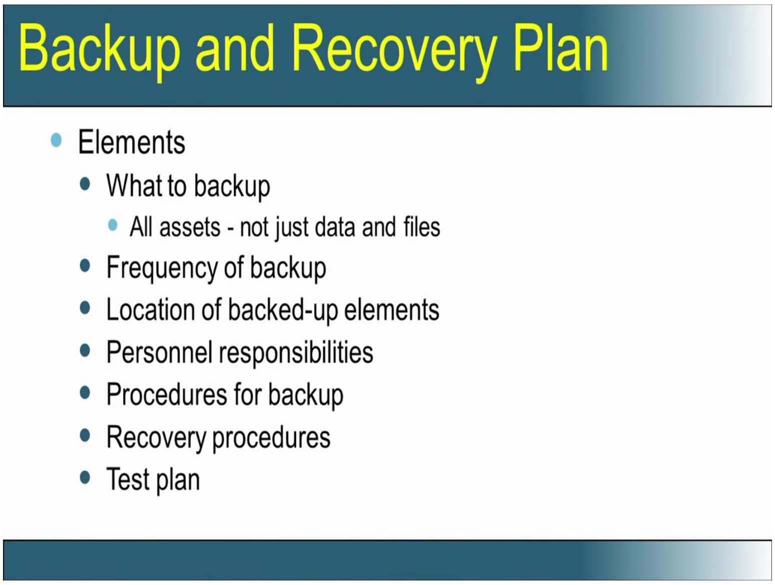
Adjust controls

Prepare security report

We will now see about the three different plans. First is the security plan. The security planning essentially involves the key elements that I have listed in the slide. First thing is we have to go and identified and evaluate what are all the assets and how are they exposed. No one… Find out what are all the… Identify and evaluate these exposed assets; we have to find – identify the threats and the level of the exposures. Then, we do what we call as an exposure analysis. Once we do an analysis of the exposure… Exposure analysis in the sense who are all using, to which level it is being used. Down the line, we will give you a very clear procedure of how to carry out this exposure analysis.

Once we perform this exposure analysis, then we can identify controls and security measures. Then, we do a cost-benefit analysis. And, based on the cost-benefit analysis, we will select controls and procedures and finally, prepare a security report. So, these are all the seven stages that go into the security plan. And, the emphasis of this planning is that, we should – this should be a plan in the sense that, the objectives and scopes should be very well defined in the sense that, you should not get bogged into many details and we need to use lot of project planning tools and get very quickly onto this plan.

(Refer Slide Time: 09:59)



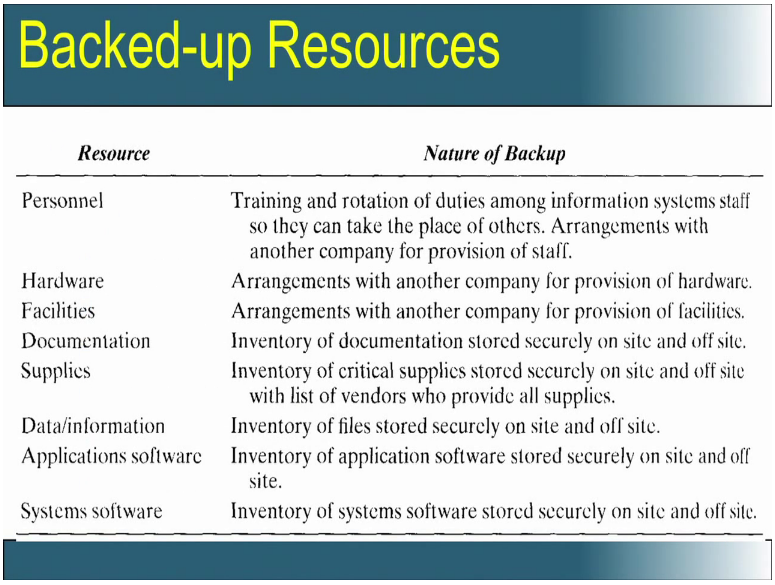
Backup and Recovery Plan

- Elements
  - What to backup
    - All assets - not just data and files
  - Frequency of backup
  - Location of backed-up elements
  - Personnel responsibilities
  - Procedures for backup
  - Recovery procedures
  - Test plan

The next is the backup and recovery plan. In this, first thing is to identify the elements that we need to backup. Should I backup all the assets? Should I backup only data? Some files, something do not need backup. If I backup all the things, for example, every action of an user if I am going to backup; then what would be the size of this backup. So, the first decision of what to backup has lot of implications on the remaining six points that you see on this slide. That will dictate how frequently should I go and back up. And then, where will the backed-up element reside? Will it reside on the data center – on the local data center or it will go onto some remote disaster recovery site? If you have lot of data to be backed up, you cannot do it very frequently, you cannot transfer it very frequently across a network.

Then, what are the personal responsibilities? What will each person do? who is responsible for which data? Who is the custodian for every data? And, what are the procedures for backup? I take yesterday's backup, I store it in some other place; and, I take today's backup; after I complete today's backup, I go and erase yesterday's backup like this. How many years should I keep a particular log? There are regulatory requirements at every stage. If it is an academic institution; I have to keep the answer script for one semester. If it is a bank, I should keep the transactions for 3 years or 6 years; it is given by the RBI in India. So, there is a very definite time period to which I can keep a log. So, these are all part of your procedures for backup. And then, if there is a failure, how do I recover, how do I rollback? Many database gives different ways of rolling back. And, the more important thing here is also the test plan. How do I test whether at every stage, things are going proper? How do I audit whether the backup is happening properly? So, all these things come as a part of your backup and recovery plan.

(Refer Slide Time: 12:32)



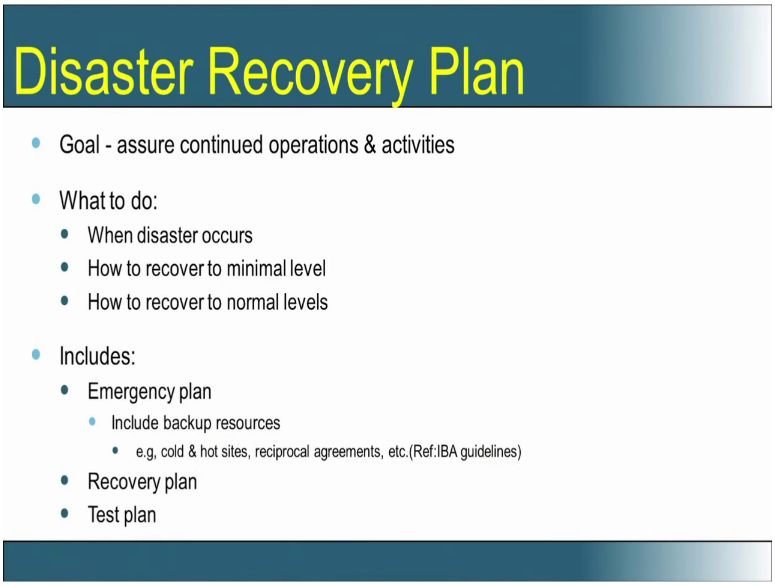
Backed-up Resources

Resource	*Nature of Backup*
Personnel	Training and rotation of duties among information systems staff so they can take the place of others. Arrangements with another company for provision of staff.
Hardware	Arrangements with another company for provision of hardware.
Facilities	Arrangements with another company for provision of facilities.
Documentation	Inventory of documentation stored securely on site and off site.
Supplies	Inventory of critical supplies stored securely on site and off site with list of vendors who provide all supplies.
Data/information	Inventory of files stored securely on site and off site.
Applications software	Inventory of application software stored securely on site and off site.
Systems software	Inventory of systems software stored securely on site and off site.

So, this is a very quick insight of what do we mean by backing up. See please note that, information asset is not just hardware and software; I am repeating it; it is people, process and technology. So, if you are looking at a perfect information security in your organization, right from your personal, your hardware, your facilities, your documentation, your supplies, your data, information, application software, system software – all of them need to be backed up. And, the most important backup is your personal. If one person is ill, your bank or your organization should not stop; the activities should go on. And, that is also security, because security again here means availability – availability to the user.

So, if suppose I say I cannot process this file today, because somebody is on leave, you are not a completely secured organization. It is very very important that there is a backup even at a personal level. The other backups are something conceivable; but, the first point is where many organizations fail; they do not have backups for every personnel. So, if one person is on leave, certain operations can either becomes slow down or certain operations are not even possible. This we see commonly in day-to-day management of organizations. So, this is one very very important thing.

(Refer Slide Time: 14:11)

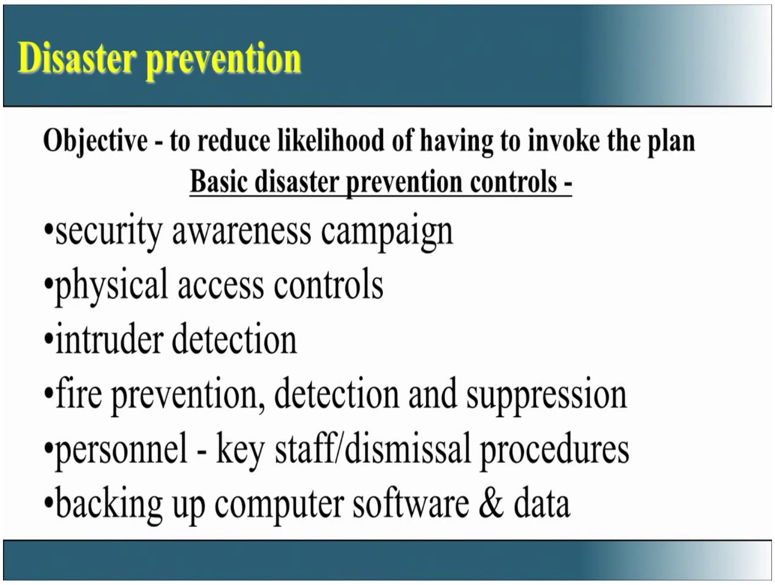


Disaster Recovery Plan

- Goal - assure continued operations & activities
- What to do:
  - When disaster occurs
  - How to recover to minimal level
  - How to recover to normal levels
- Includes:
  - Emergency plan
    - Include backup resources
      - e.g, cold & hot sites, reciprocal agreements, etc.(Ref:IBA guidelines)
  - Recovery plan
  - Test plan

That last is about the disaster recovery plan. Suppose there is a disaster; first and foremost – when disaster occurs, what should be the first aid? How to recover to the minimal levels? Then, how to recover to the nominal level? Then, how do I come back in full glory? So, this disaster recovery plan in turn will have again three plans: emergency plan, and that is the first; 2 – how to recover to minimal level and to nominal levels? And then, the recovery plan again – how to come back to the full glory. And, another thing here is very much necessary is the test plan. Even regulatory authorities in the case of the banking segment, RBI has clear guidelines about disaster recovery; they call it as a emergency drill. So, the test plan is one mandatory requirement by the regularity body, where you do these drills that, there is a emergency, there is a disaster; how do I go and recover from this disaster. So, you simulate a disaster. So, this is sometimes called DR drill – disaster recovery drill. And, that is part of your test plan. So, it should be stated how frequently will I do this test, etcetera.

(Refer Slide Time: 15:37)



Disaster prevention

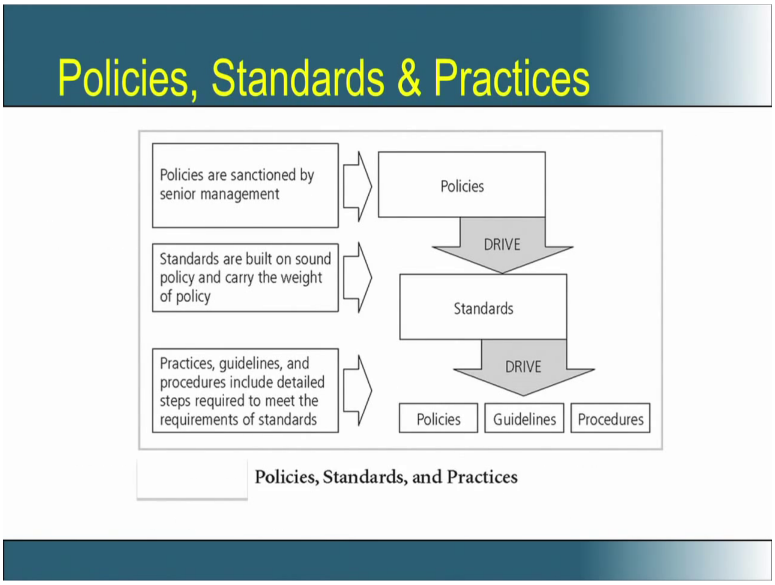
Objective - to reduce likelihood of having to invoke the plan

Basic disaster prevention controls -

- security awareness campaign
- physical access controls
- intruder detection
- fire prevention, detection and suppression
- personnel - key staff/dismissal procedures
- backing up computer software & data

So, to conclude this particular session, we will make this. Please note that, disaster prevention means to reduce the likelihood of having to invoke the plan. So, when we look at all these, there are three plans that we need to keep up: the security plan, the backup and recovery plan, and the disaster recovery plan. And, all these things people should be educated; there should be an awareness campaign; there should be lot of physical access control; there should be intruder detection, fire prevention, detection, suppression, personnel training, personnel training of… and appointment of key staffs. And, when you dismiss someone, how do you handle those scenarios and backing up. All these things together are basically to be targeted in this class.

(Refer Slide Time: 16:30)



Policies, Standards & Practices

Policies are sanctioned by senior management

Standards are built on sound policy and carry the weight of policy

Practices, guidelines, and procedures include detailed steps required to meet the requirements of standards

Policies, Standards, and Practices

Now, in the next session, we will go and start talking about each of these plans in more detail.