ISMS Implementation Guide

By Vinod Kumar Puthuseeri
Information Security Consultant

Table of Contents

Objective

This paper can serve as a guideline for the implementation of ISMS practices using BS7799 / ISO 27001 standards. To give an insight and help those who are implementing this for the first time and for those who will be coordinating with external consultants for ISMS implementations in their organizations.

Scope

This document will cover the requirements from an audit point of view, methods and tips on implementing ISMS practices.

Standard

BS7799 / ISO 27001

BS7799 is a British Standard that addresses Information Security in all areas including Physical Security. BS7799 was incorporated with some of the controls from ISO 9000 and the latest version is called ISO 27001.

There are 11 chapters in the ISO 27001 version.

| 2000 Edition / BS 7799		2005 Edition / ISO 27001
	Security Policy	Security Policy	
	Security Organization	Organizing Information Security	
	Asset Classification and Control	Asset Management	
	Personnel Security	Human Resource Security	
	Physical & Environmental Security	Physical & Environmental Security	
	Communications and Operations Management	Communications and Operations Management	
	Access Control	Access Control	
	System Development and Maintenance	Information Systems Acquisition, Development and Maintenance	
		Information Security Incident Management	
	Business Continuity Management	Business Continuity Management	
	Compliance	Compliance	

Note: This is an extract from the BS document – Focus on ISO 27001:2005 standard, which can be downloaded from:
http://asia.bsi-global.com/InformationSecurity/ISO27001+Guidance/FocusOnISO27001Jan06.pdf
This document also illustrates the changes made in the controls and the comments.

<u>The CIA triad</u>

The framework addresses three core factors of all the Information assets.
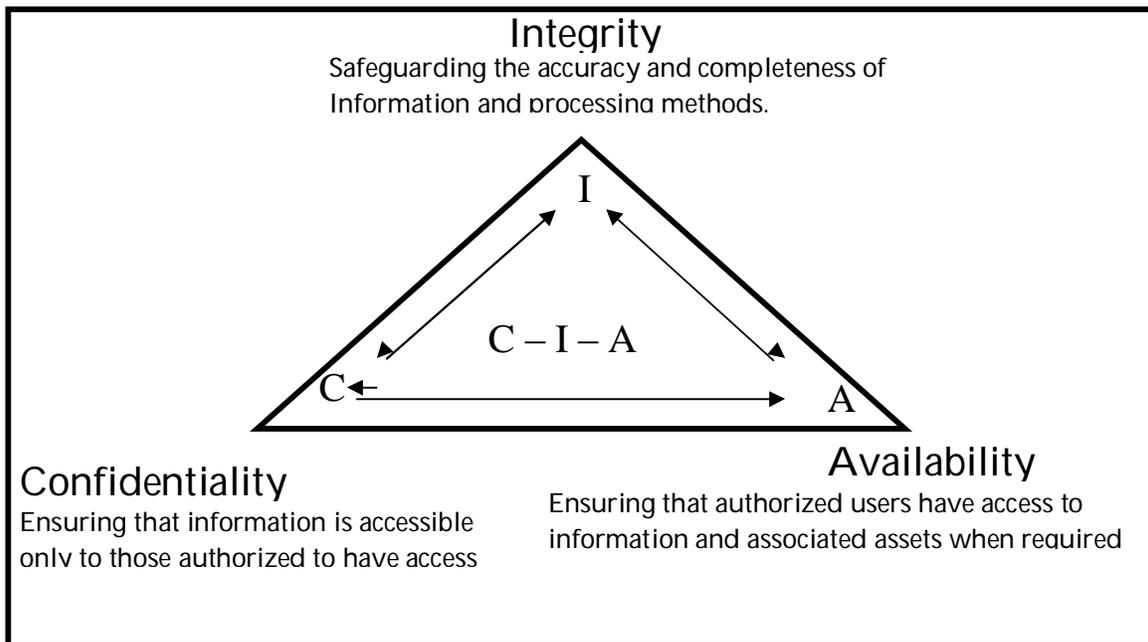
As mentioned above ISO/IEC 27001 standard has 11 Domains, which address key areas of Information Security Management.

<div align="center">

Security Policy
Organizing Information Security
Asset Management
Human Resource Security
Physical & Environmental Security
Communications and Operations Management
Access Control
Information Systems Acquisition, Development and Maintenance
Information Security Incident Management
Business Continuity Management
Compliance

</div>

BS 7799 (ISO 27001) consists of 134 best security practices (covering 11 Domains which was discussed above) which organizations can adopt to build their Security Infrastructure.

Even if an organization decides not go in for the certification, BS 7799 (ISO 27001) model helps organizations maintain organizational security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement.

PDCA Model

The formula, PDCA (PLAN …DO …CHECK and ACT) is adopted in BS 7799 and this is a good place to either start or review the progress of the implementation.

PDCA Model
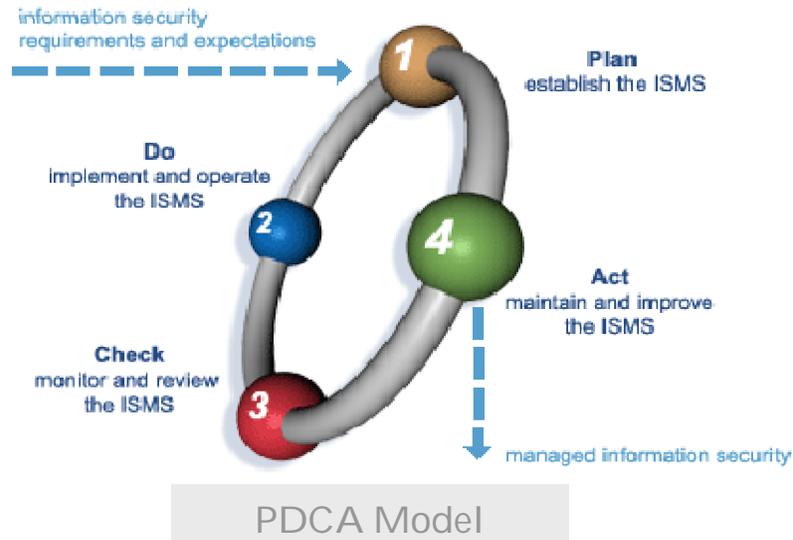
The Plan, Do, Check and Act framework is cyclic and has to be continuously done for long run and with the solid backing of the management.

It is recommended that the ISMS be based on the Deming Wheel model introduced in BS7799-2002 Part 2 (PDCA - Plan, Do, Check & Act), which is a de-facto methodology and ensures that the correct components are engaged, evaluated, monitored and improved on a continuous basis

Benefits

Benefits include:

  ü Improved security throughout the organization
  ü Improved security planning
  ü Demonstrates company's commitment in protecting information
  ü Security management effectiveness
  ü Ongoing protection over Information
  ü Less risk when dealing with partners
  ü Improved customer, employee and partner confidence
  ü More realistic and manageable auditing
  ü Reduced liability over information

Management

Management Commitment

The requirement for BS7799 / ISO 27001 implementation or certification is mainly driven by external pressure, like a client requirement. The management will only be worried of the above mentioned aspects and first step they would do is to allocate a budget for this project and ask the IT or QMS or for that case any department to complete the project.

The goal should be, to make the management understand the actual requirement for this implementation and also project the results / benefits of this project. Sometimes (depending on your nature of business) you do not even require to go in for the certification process. At times you might even not require certifying or implementing the process at all your branches.

The best method to project requirement and results to the management is to map the any of your requirement into cost. "Time is money" and so if there is any disruption of service it will directly impact the business. Let us look at a case study here:

Case Study

There was a virus outbreak in an organization that affected just one project and it consists of 4 developers. The entire systems were brought to a halt and there was no way to work until the virus was completely cleared from the systems. The systems group with a two member team took about 3 hours to clear the virus and bring back the systems into operations. Let us now calculate the amount of loss the organization has gone through:

Number of resources affected: 4 developers + 2 systems group member = 6 resources

Developer
Price / hour: Rs.1350/- (for example)
Time lost: 3 hours
Loss: Rs. 16200

System group
Price / hour: Rs.900/- (for example)
Time lost: 3 hours
Loss: Rs.5400

The total cost to the organization by just this event is Rs. 21,600/-. But again the developers need to spend another 3 hours to complete the job that was not done

during the downtime. So, I would say the total cost lost to the organization is Rs.37800/-. In addition we will also loose the rapport with our clients.

The management will understand figures; whether projected using the cost or the percentage of failures. Before we begin with this project, it is very important or let's says it is mandatory that we make management the actual requirement. Again we will require having a commitment from the management to support this implementation process throughout the project as this will be an organization wide effort rather than just the IT department.

"Information Security is everyone's responsibility"

Implementation Process

Let us now look at the various points that need to be covered under each domain. A brief explanation is given and examples quoted wherever necessary.

The team We will require forming a team to take this forward. We will require having a person who will be the primary interface between the implementation team and the senior management. Let us name this person as the Chief Information Security Officer (CISO). The CISO will be responsible in getting formal approvals from the management and also should be capable of taking decisions on behalf of the management.

We will also require having a project manager who will be overall in charge of the project and will be reporting to the CISO. Let us name his as the Information Security Officer (ISO). The implementation team members can be selected from every team / group / department within your scope, which will help in a smooth implementation process.

Define the Scope ISMS can be implemented for just a department, for just one floor of an organization, for the entire or part of an organization. You will require having a discussion with the senior management and pen down the areas where you would like to implement ISMS practices. This has to be clearly defined in your Information Security Policy document.

Business process study of individual departments: We have already identified the departments within the scope and also we have one member from each department to be a part of our implementation team. Have a discussion with these team members to understand the process involved in carrying out their task within their department.

For ex: let us take one part of the HR department. If we looking at the hiring process of the HR department, there would be different levels of interviews,

every interview will have it own standards and methods, after the interviews are over, there will be a offer given and on acceptance the candidate joins the organization. Once the joining formalities are over, there will be a background check done of the employee.

This process of hiring an employee, which is a part of the HR department need to be documented and is known as Business Process study and it has to be done for each and every department within the scope. The process of having the business process study document is not a mandatory requirement as ISO 27001 standards, but will help in the later stages for identifying the assets involved in carrying out their tasks and also to value those assets.

Risk Assessment

Asset Inventory Information can exist in different forms and those that hold this information are known as information assets. This can be

- ü Information / Data asset
- ü Technology Asset
- ü People Asset
- ü Service Asset

All the information assets of these departments should be identified and documented. On identifying these assets it will be a good practice to label these assets. A format needs to be defined to label all the assets within the organization.

Every asset will have an asset owner and an asset custodian. We will require documenting the asset owner and the asset custodian of a particular asset.

For ex: Let us take the case of a critical server in the organization. The owner of the server (hardware) would be the server group, the application owner might be the application group and the owner of the data residing in the server might be the system development group. This will vary from server to server or organization to organization or might be the same. It is also possible that the owner and custodian of the hardware, software and data be the same. This needs to be identified and documented.

Asset Value Asset value can be defined by looking at confidentiality, integrity and availability of an asset. Let me give you an example which will be easier to understand.

Let us take the mail server of the organization. The asset owner of the server and the custodian of the data been the server group and asset owner of the data been everyone who uses the server. Let us define a scale of 1-5 to record and assign a value to the owners and custodians views.

Confidentiality
Q. What if an intruder or another employee of a lower access level gets to read confidential top management mails?
Answer 1: It is very critical. Since the top management exchanges a lot of information through emails.

Answer 2: It is not very critical. Since all our communication is encrypted using digital signatures, there is a very rare chance of information leakage.

For answer 1 the confidentiality value is 4
For answer 2 the confidentiality value is 2

Integrity
Q. What if an intruder or another employee tries to modify the contents of the mail and the mail delivered is something different. For ex: The CEO sends out a mail to the CFO to donate Rs.1, 00,000 for a charity. Someone in between tampers the mail and changes the amount to Rs.7, 00,000 and give his account number.
Answer 1: It is very critical.

Answer 2: It is not very critical as all the internal and external mail communication are encrypted

For answer 1 the integrity value is 4
For answer 2 the integrity value is 2

Availability
Q. What happens if there is a hardware failure and the server is not available to the organization…???
Answer 1: It is very critical. We might even have the mails coming in not been delivered. There might be a data corruption and there is a possibility of users losing their mails.

Answer 2: It is not very critical. My servers run on redundancy and I have a backup MX record created. If there is a hardware failure, the backup server and MX record will take over and there will not disruption to the services.

For answer 1 the availability value is 4
For answer 2 the availability value is 2

Now let us arrive at the asset value by using a simple method. Note: various other methods are also available, this is just an example.

Asset value = Confidentiality + Availability + Integrity

Mail Server Value = 4 + 4 + 4 = 12 (for very critical)
Mail Server Value = 2 + 2 + 2 = 8 (for not critical)

The next step is to identify the risk value of this particular asset. Let us see how to arrive at the risk value.

Risk Value The risk value for an asset has to be determined by identifying the possible threats that can impact the CIA of the asset, how much impact will it cause, what is the frequency of the impact and the asset value.

Let us take the mail server as mentioned above for this example. We have already identified the asset value, now we need to list down the threats to the mail server.

- ü Power failures
- ü Hardware failure
- ü Fire
- ü Virus attacks / Malicious code injection
- ü Intruders (Hacking), Denial of Service (DoS attack)
- ü Mail accidentally sent to a different recipient
- ü Data corruption / data loss
- ü Unauthorized access
- ü Link failure
- ü Natural calamities

Business Impact Analysis (BIA)

BIA is performed to analyze the impact on the system due to various unprecedented events or incidents. Various failure scenarios and its possible business impacts are analyzed. This includes technical problems, human resources and other events.

Now you might ask me, we have already identified the asset value which is based on the threats and vulnerabilities, that will show us the impact on business. Why do we need to have another analysis…???

BIA is different from Risk assessment. Risk Assessment will identify the possible threats and vulnerabilities and how those will impact the asset and business. The asset value shows how critical is that asset to the organization.

BIA is based on time. If there is a server crash, let's take the mail server as per the example above, how much time can the organization go without an email server. This is derived by doing the business impact analysis.

The different steps to be followed in determining the business impact is as shown below:
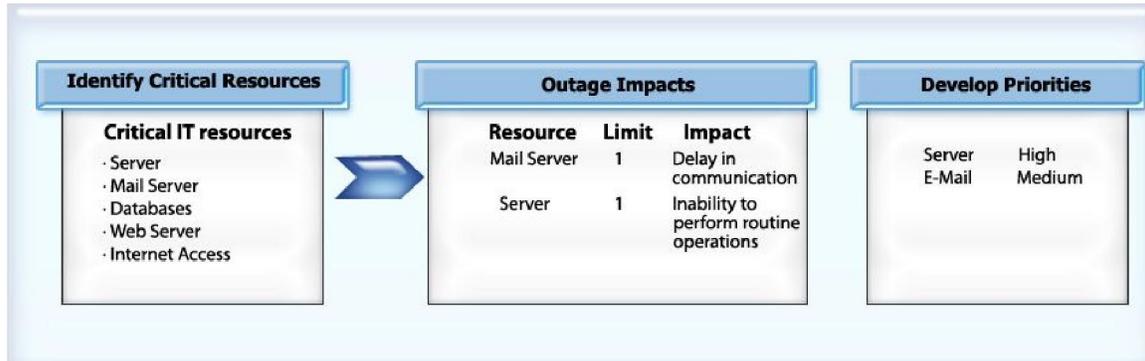
Identify the critical resource, which has already been done during accumulating the assets and deriving the asset value. List down all possible impact to business and prioritize the assets. In this example of deriving the BIA, we shall use a scale of 1 to 5 and since mail server is critical to the organization, we shall take 4 as the BIA value.

Probability of Occurrence

The probability of occurrence is required to understand the frequency at which such failures occur. This is based upon previous experiences and also looking at the current implementation. The probability of occurrence is measured on a scale of 0.1 to 1. Refer to the table as mentioned below.

Probability of Occurrence	Probability Rating
Low	0.1
Medium	0.4
High	0.7
Very High	1

For this example, let us consider the probability of occurrence to be rated at Medium which will have the value as 0.4. Let us now see how we can arrive at the risk value.

Risk Value = Asset value * Business Impact * Probability of Occurrence

Risk Value = 12 * 4 * 0.4 = 19.2

Risk Assessment Tools

Various other tools that can be used for risk assessment are

- Asset Track -- http://www.libsuite.com/asset_track.htm
- CRAMM – http://www.cramm.com
- Riskwatch – http://www.riskwatch.com
- RA2 art of risk -- http://www.bsi-global.com/ICT/Security/bip0022.xalter
- Exrisk -- http://www.ezrisk.co.uk/
- Risk Point -- http://www.riskpoint.com.au/standards.html

Why identify the risk value

Here we have taken the example of a mail server and determined the risk value. In cases where you do a risk assessment on a desktop or some templates, the risk value might be much lower. By this method you will be able to decide as which assets need to be considered for risk treatment in the next phase and the rest can be ignored. This is done because, if we do a risk treatment on assets that has a low risk value, the money spent to mitigate risk on those assets might be much higher than the cost of the asset on the loss it could cause to the business.

We have the risk value and have decided to do a risk treatment for this asset as it is a very important asset for the organization.

Risk Management

Let us see how we can eliminate or reduce the risk due to the above mentioned threats, by mapping each threat to an available ISO 27001 standards.

Threats	ISO 27001 Controls	Implementation
Power Failures	A.9.2.2	UPS, generator
Hardware Failures	A.9.2.4	AMC's
Fire	A.9.1.4	Fire Extinguishers, Sprinklers
Virus, Malicious Code injection	A.10.4.1	Anti-virus, Anti-spam, spy ware removal tool
Hacking, DoS attacks	A.6.2.1, A.6.2.3, A.10.6.1	Perimeter Security Devices, Adequate Network controls
Mail accidentally sent to a different recipient	A.10.8.4	Digital Signatures
Data Corruption / Data Loss	A.10.5.1	Backup
Unauthorized access	A.11.2.2, A.11.2.4, A.11.5.2	Active Directory, User access rights

| Link failure | A.14.1 | Business Continuity Plans |
| Natural Calamities | A.9.1.4 | Identification of such areas, Insurance, Disaster Recovery sites |

Above is the example of how we can map each threat identified to ISO 27001 controls and also to find how to minimize the risk.

Deciding Assets for Risk Mitigation

Having the asset value and risk value determined, the management should now decide on assets that have to be considered for risk mitigation. This is mandatory because, some of the controls that need to be implemented to mitigate risk might cost the organization more than the asset value. Assets that can be recreated (such as templates, standard forms etc) without causing any impact to the business can to be eliminated from risk mitigation process.

Different Methods of Handling Risks

Risk Acceptance: To accept the risk and continue operating or to implement controls to lower the risk to an acceptable level. We need to give a high priority to the business requirements, while also looking at how to safeguard information. There are instances where we will require accepting certain risk and seeing to that the business requirements is met.

For example: Due to some testing purpose who need to move one of your servers to the DMZ zone for a particular period of time. Since this testing is mandatory, it can be considered as an acceptable risk for that period. But this should be agreed by the management and the asset owners.

Risk Avoidance: To avoid the risk by eliminating the risk cause and / or consequence. If there is an old system (Windows 98 running some proprietary application), which cannot be patched for the current vulnerabilities and is of not much use to the organization can be eliminated by switching off the machine.

Risk Limitation: To limit the risk by implementing controls that minimizes the adverse impact of a threat's on an asset. By implementing anti-virus server in the organization does not ensure that the assets will be protected from virus attacks. This is a method of minimizing the risk from known virus attacks.

Risk Planning: To manage risk by developing a risk mitigation plan that prioritizes, implements and maintains control. We foresee some of the risks due to natural calamities. For the case of fire, it is recommended to have fire drills at regular intervals, have fire extinguishers placed at fire prone areas; marking fire

exists and keeping those paths clear with no obstructions, have documented procedures and guidelines on operations of fire extinguishers and how to act during a fire.

Research and Acknowledgement: To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability. As mentioned before, if you have a system that is outdated or having some proprietary applications, it might not be possible to patch the system for vulnerabilities, as the patch might affect the operation of the software. In such cases it is recommended to either run the application as it is and treat it as an acceptable risk or research to find if there are any alternative methods to patch the particular application.

Risk Transfer: To transfer the risk by using other options to compensate for the loss, such as purchasing insurance. Risk can also be transferred by having a contract with your vendors. In the means of annual maintenance contract (AMC's) or any other agreement of having spares at your location.

Statement of Applicability (SOA)
SOA is a document that states all of the ISO 27001 controls. This requires identifying those that are applicable and give a justification for choosing that particular control. A justification also needs to be given for that control that has not been chosen for implementation.

This SOA document will be provided to clients and external trusted authorities on demand, for them to identify the level of implementation of security practices in the organization. The headers of the SOA document can be as mentioned below. This is just an example

| Control Reference	Description	Implementation	Justification
A.9.2.2	Fire Supplies	Yes	Have implemented UPS systems and also a dedicated generator for the entire building
A.10.4.1	Malicious Code	Yes	Have implemented a centralized anti-virus server that caters to the entire organization. Anti-virus policy

			document is also available.

Some of these controls require policies to support the implementation. As mentioned above anti-virus policy is a policy that defines how anti-virus is deployed across the organization, what are the tools used and how is it monitored. Make sure all the policies are in place and we will also require documenting the operating procedures of all the assets in the organization.

Business Continuity Plan & Disaster Recovery (BCP & DR)

Business continuity planning and disaster recovery planning are vital activities. Prior to creation of the plan itself, it is essential to consider the potential impacts of disaster and to understand the underlying risks. I shall not go in depth details of preparing and implementing a DCR and DR as this is a vast subject by itself.

Process
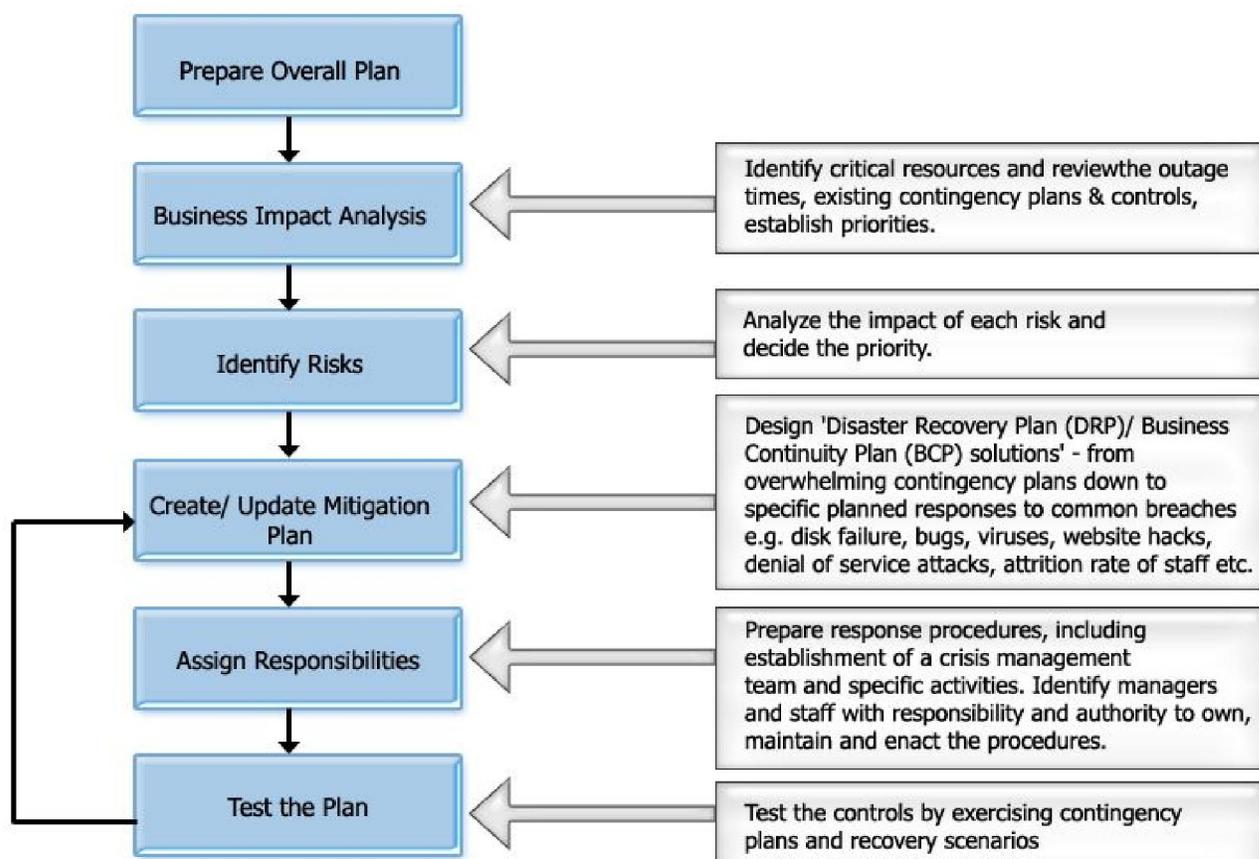
Business Impact Analysis

Refer to BIA topic

Audit

This section we shall talk about how the audit is conducted, what are the various areas that we need to concentrate for both internal as well certification audits. The external audit procedure will vary and depend on the external auditors. The common method is as mentioned below:

Pre-Assessment Audit (Adequacy Audit)
This step is optional, but is highly recommended if you are doing the implementation for the first time. You can have a minimum of two months between the pre-assessment audit and the certification audit. This step will ensure if you are ready for the certification audit.

Document Review
The first step in the certification audit process is the document review. Below are the documents generally audited:

- ü Policy documents
- ü Policy statement
- ü Risk assessment report
- ü Risk assessment procedure
- ü Mapping of threats to the assets
- ü Statement of applicability
- ü Mapping of risk assessment report to the statement of applicability
- ü BCP, BCP testing procedure and test results
- ü Technical audit reports (Vulnerability Assessment and Penetration Testing reports)
- ü Metrics if any
- ü Procedure and guideline documents

On Floor Audit
The auditor will look for physical security as he walks through the organization premises for auditing user awareness as well as individual departments within the scope. All departments with the scope should have their policy, procedure and guideline documents updated.

Internal Audit
An internal audit should be conducted before the start of the project. This will project the gaps and you will understand where you stand. Further conduct two more internal audits, one in the middle of the project and one just before the

document review. Document you internal audit schedules for the next one year, as this is one of the documents that will be asked for during the document review.

Following are some of the common areas for internal auditing. In additional you will require auditing your departments, depending on their policy and procedures. This will vary and depend on organizations.

<u>Desktop Audit</u>

Desktop audit is primarily done to check if users have any illegal contents on their desktops. Such as .mp3 files, video files, .jpeg, .jpg and .gif files that can have pornography materials. You can also audit their mailboxes by looking for mails with huge attachments, jokes been received and forwarded to other colleagues (all these must be mentioned as a violation in your organization email policy).

Users are very smart and so you should do a search for any .pst files (if using outlook mail client) to see if there are any personal files available. Usually users copy all illegal mails, jokes and mails with pictures of huge attachments to a personal folder and offload the same from the mail client, especially when there is an audit happening in the organization.

<u>User Awareness Audit</u>

User awareness audits are conducted to check the level of awareness in the employees. Whatever technical solutions have be implemented, unless the user awareness is not strong, it will be biggest threat to the organization.

While you conduct an audit on the user awareness, ask questions about the following:

- Organization policy statement
- Email Policy
- Internet usage policy
- What is meant by tailgating..?? What do you do when you see someone tailgating…???
- What do you do when you see someone not in their seat and the machine has not been locked…???
- What do they do when they sight a person who within the organization premises without a valid organization ID card…???
- Who are the ISO (Information Security Officer) and CISO (Chief Information Security Officer) of the organization…???
- Have you been through the corporate user awareness program on Information Security…??? If no, why…???

<u>Technical Audit</u>:
I would suggest that vulnerability assessment and penetration testing to be conducted by external vendors. We should not build the network and test it ourselves. It would be like cooking, tasting and certifying that the food is good by the same person.

Keep in mind to inform the vendors that these testing will be done only during a pre-determined schedule and also no vulnerabilities will be exploited. Exploiting vulnerabilities might bring the targeted services and you will be held responsible for the same.

If you have a method of logging and monitoring your internet traffic, keep an eye on it and see if there is any access to illegal sites.

<u>Social Engineering</u>
Social engineering is a method of extracting information from people (in this case the employee) to intrude into your premises or network. Social Engineering tests can be conducted by making telephone calls, sending emails etc.

Get a list of selected users from various departments like finance, development, operations, admin, HR, your CEO's assistant and never forget to include the front office executive.

Hand over these names along with the contact number to an external consultant. Request the consultant to make calls and ask them for information pertaining to their departments. This can be done by your team too, but sometime people recognize voice and the pattern in which an individual speak.

Suppose you call the personal assistant of the CEO and request for an appointment. The PA should do be disclosing information like the CEO is not in town and he/she is in US / board meeting etc. The intruder can also ask for the mobile number of the CEO since he/she is not in office. This is basically giving out information which is not really required to go out of the office.

Another method of conducting this audit would be to host a server somewhere outside your network and send a link to selected users via email and ask them to click on the link to download a critical patch from some vendor (maybe Microsoft). The link to should point to the server outside your network and once the user clicks on the link it should give out a page of Information Security breach and its impact.

Social Engineering is an art and human beings comment cause of the following reasons

- Scarcity: Manipulates employees by building a sense of urgency

- Authority: Scams the worker based on the premise of power. As an example: "Hi, is this the help desk? I work for the senior VP and he needs his password reset in a hurry!"

- Liking: Preys on the fact that we tend to do more for people we like even if that means bending the rules.

- Consistency: People like balance and order. As an example, when people ask how we are, we tend to respond, "Good!"

- Social validation: Based on the idea that if one person does it, others will, too. As an example: Have you ever seen a bartender's tip jar that's full of dollars? It may make you think that if everyone else is tipping, so should you!

- Reciprocation: If someone gives you a token or small gift, you feel pressured to give something in return

The above points are an extract from the internet just to give you an idea of how an attack can be performed. Try this at your organization and see how much information can be extracted.

Physical Security

Apart from walking around and viewing the infrastructure, try to check some of the locations where you can get some confidential information. Try going to one of your common printer location, I am certain in most of the organizations the user would have fired the print, but would have never collected the same. You will find a pile of documents near the printers.

Also try some of the dustbins. Check to see if critical departments have paper shredders at their department location. Some of the organizations have the habit of piling up the documents to be shredded and the office boy does it once everyday during COB (Close of business). Now you need to check if the office boy actually shreds the papers or is some is carried away.

Some of the crucial points to check on physical security are:

- Fire Exits signs

- Fire extinguishers maintenance labels
- Placement of fire extinguishers
- UPS placement and maintenance
- Generators for the building or the organization
- Distance between data and power cables
- Logging of access to data center/server room
- Entry and exit points
- Physical security placements.
- Check the inward and outward registers of visitors and materials

This is just a short list. But as you walk along the premises, I am sure of your finding many of these sorts.

Post Audit Check
- Asset tags – Make sure all your assets is been labeled as per your policy

- Mechanism to assess and improve user awareness among employees – There should be a mechanism, at least maintain records for the user awareness training conducted

- Mechanism (procedure) to record the security incidents and their solutions – There should be a process to record security incidents found and reported by users, action taken for those incidents and learning from those incidents need to be documented.

- Mechanism to store the logs of servers and other monitoring tools for further reference – Log retention need to defined and practiced

- Back-up and restore procedures to be in place. Test of restoring data has to be practiced and documented.

- BCP needs to be documented. Any test done to check the BCP need to be documented with test results.

- DR site should be defined and documented

- All cabling (power & data) should be adequately protected

- License management should be demonstrated – License management using some tools or recorded in an excel file should be produced. Audits will be conducted to check if the installation of software is same as mentioned in the license management document.

- Audit reports of VA, PT and other audits conducted in the organization should be adequately documented, measured and improvements should be projected for auditing

- Patch management and anti-virus management is recommended to be centralized and a dedicated person be assigned to monitor this area. A random audit should be conducted to check if any of the machines has been omitted by the system of any anti-virus or patch updates

User Awareness

There are different methods to pass on the information to end users. Some of which have been explained below.

Train the trainer approach: At times it is very difficult to reach every user in an organization (usually organization with more than 500 employees) and also tracking will be a tedious process. This method will be used to train a set of people (generally in the level of middle management) and they take the responsibility of training their team.

Without train the trainer approach: This method is used generally in smaller organizations. Here the training program will conducted to each and every employees of the organization by the same team of trainers.

Training Materials: Preparation of training materials should depend on the targeted audience. Split the organization based on the following:

§ Senior Management
§ Middle Management
§ End Users

If you have a training session for the senior management, make sure you also include some statistics of your vulnerability report, comparison between previous reports. The main focus should be to show the improvements that you have achieved through this implementation.

For the end users, consider shooting a shot film by having some of your in-house members to act for the video. This will be very interesting and I am sure you will have volunteers coming up for this purpose. You can also have pictures taken in around your premises that pose as examples for the common security breaches and use those pictures can be used as your screen savers. Handbook, hand-outs and Information Security bulletin are additional means to spread information to all employees.

Reference

1. BS ISO/IEC 27001:2005 Information technology – Security techniques
2. Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards and Technology
3. Internet

Declaration

All contents in this document are prepared by me with my personal experience of ISMS implementation and auditing. The pictures and quotes have been taken the internet. Kindly note that the document is just guidance to the implementation of ISMS practices in an organization. Risk assessment illustrated is one method and there are other methods that can be followed.

Disclaimer

The editor is unable to accept any legal liability for any consequential loss or damage, however caused, arising as a result of any actions taken or not taken on the basis of the information contained on this article.

Copyright

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Contact

Vinod Kumar Puthuseeri
Email: vinodjis@gmail.com, vinodjis@hotmail.com, vinodjis2@yahoo.co.in

GNU Free Documentation License

http://www.gnu.org/licenses/fdl.txt