Lab assignment 3

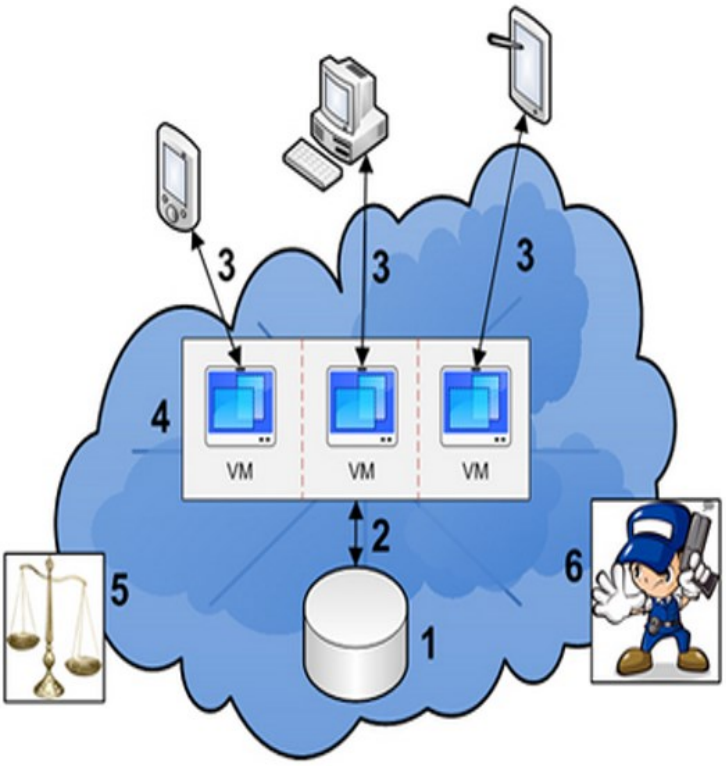
Information security analysis and audit

Name: Abhay Rathi

Reg. No: 20BCE2905

Lab slot: 31+32

1.



Discuss about the various events/incident/alert that can be audited by an ISAA team on the six vulnerability points mentioned in the cloud set-up?

1.Authentication: Authentication is the process of verifying the identity of a user, device, or other entity. This can be done through the use of credentials, such as a username and password, or biometric data, such as a fingerprint or iris scan. All authentication events/incidents/alerts should be audited by the ISAA team. This includes successful and failed authentication attempts, as well as any attempts to bypass authentication mechanisms.

2. Authorization: Authorization is the process of determining whether an entity is allowed to access a particular resource. This can be done through the use of permissions, which specify what an entity is allowed to do with a resource. All authorization events/incidents/alerts should be audited by the ISAA team. This includes successful and failed authorization attempts, as well as any attempts to bypass authorization mechanisms.

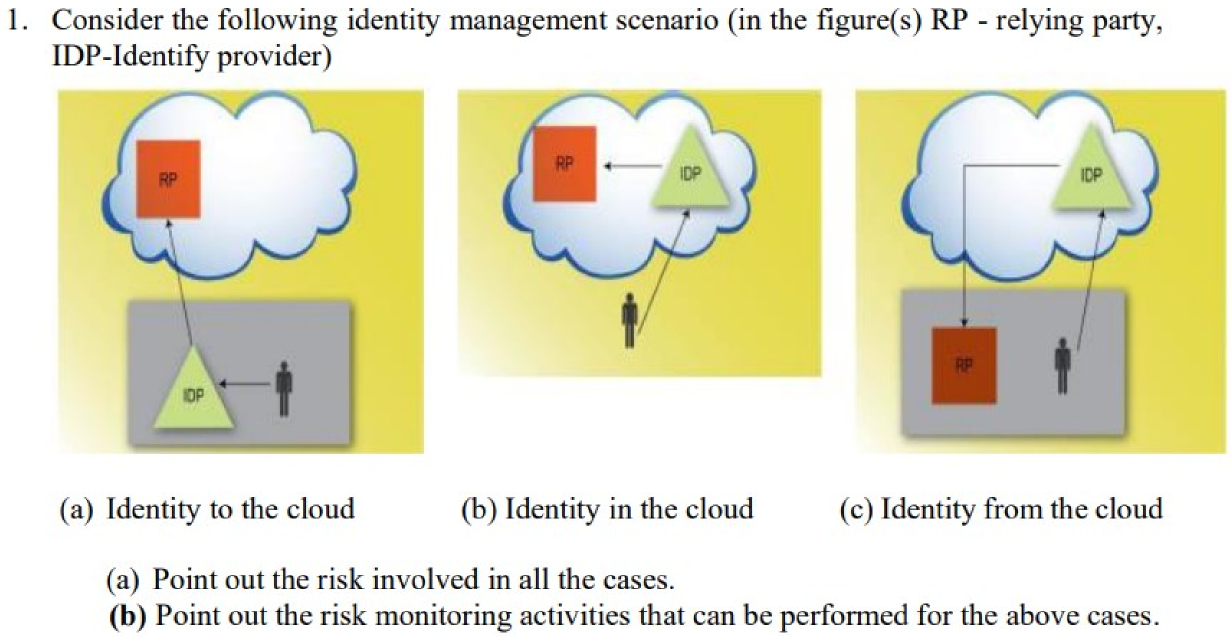
3. Access Control: Access control is the process of controlling who is allowed to access a particular resource. This can be done through the use of permissions, which specify what an entity is allowed to do with a resource. All access control events/incidents/alerts should be audited by the ISAA team. This includes successful and failed access control attempts, as well as any attempts to bypass access control mechanisms.

4. Data Protection: Data protection is the process of safeguarding data from unauthorized access. This can be done through the use of encryption, which makes it difficult for unauthorized entities to read the data. All data protection events/incidents/alerts should be audited by the ISAA team. This includes successful and failed data protection attempts, as well as any attempts to bypass data protection mechanisms.

5. System and Network Configuration: System and network configuration is the process of configuring systems and networks to be secure. This can be done through the use of security policies, which specify what an entity is allowed to do with a resource. All system and network configuration events/incidents/alerts should be audited by the ISAA team. This includes successful and failed system and network configuration attempts, as well as any attempts to bypass system and network configuration mechanisms.

6. Security Incident Management: Security incident management is the process of responding to and managing security incidents. This can be done through the use of incident response plans, which specify how an organization will respond to a security incident. All security incident management events/incidents/alerts should be audited by the ISAA team. This includes successful and failed security incident management attempts, as well as any attempts to bypass security incident management mechanisms.

2.



1. Consider the following identity management scenario (in the figure(s) RP - relying party, IDP-Identify provider)

(a) Identity to the cloud (b) Identity in the cloud (c) Identity from the cloud

(a) Point out the risk involved in all the cases.
(b) Point out the risk monitoring activities that can be performed for the above cases.

A: RISK INVOLVED IN ALL THE CASES

1.1 Theft or loss of intellectual property

An lot of data uploaded by companies to cloud-based file management services contain sensitive data. The analysis found that companies face the risk of having their intellectual property stolen.

1.2 Compliance violations

A state of non-compliance with any of these bodies lands companies in a lot of trouble. To mitigate this risk, companies should always use authentication systems for all the sensitive data in the firm.

Even tech giants like Facebook have been victims of resource exploitation due to user error or misconfigurations. Keeping employees informed about the dangers and risks of data sharing is of at most importance.

2.1 Malware attacks

Cloud services can be a vector for data exfiltration. As technology improves, and protection systems evolve, cyber-criminals have also come up with new techniques to deliver malware targets. Attackers encode sensitive data onto video files and upload them to YouTube.

2.2 End-user control

When a firm is unaware of the risk posed by workers using cloud services, the employees could be sharing just about anything without raising eyebrows. Insider threats have become common in the modern market. For instance, if a salesman is about to resign from one firm to join a competitor firm, they could upload customer contacts to cloud storage services and access them later.

3.1 Attacks to deny service to legitimate users

You are most likely well aware of cyber-attacks and how they can be used to hijack information and establish a foothold on the service provider’s platform. Denial of service attacks, unlike cyber-attacks, do not attempt to bypass your security protocol. Instead, they make your servers unavailable to illegitimate users.

3.2 Shared vulnerabilities

Cloud security is the responsibility of all concerned parties in a business agreement. From the service provider to the client and business partners, every stakeholder shares responsibility in securing data. Every client should be inclined to take precautionary measures to protect their sensitive data.

Loss of data

Data stored on cloud servers can be lost through a natural disaster, malicious attacks, or a data wipe by the service provider. Losing sensitive data is devastating to firms, especially if they have no recovery plan. Google is an example of the big tech firms that have suffered permanent data loss after being struck by lightning four times in its power supply lines.

Increased customer agitation

A growing number of cloud service critics are keen to see which service providers have weak security protocols and encourage customers to avoid them. Most of these critics are popular around the internet and could lead to a poor impression of your firm in a few posts.

If your customers suspect that their data is not safe in your hands, they not only move to competitor firms but also damage your firm’s reputation.

RISK MONITORING ACTIVITIES

1. Ensure governance and compliance is effective:
A majority of companies have already established privacy and compliance policies to protect their assets. In addition to these rules, they should also create a framework of governance that establishes authority and a chain of responsibility in the organization.
A well-defined set of policies clearly describes the responsibilities and roles of each employee. It should also define how they interact and pass information.

2. Auditing and business procedures
Every system in an organization requires a regular audit. In fact, it is of utmost importance that firms keep their IT systems in check in case of malware and phishing attacks.
An IT system audit must also check the compliance of IT system vendors and data in the cloud servers. These are the three crucial areas that need to be frequently audited by cloud service customers:
i. Security in the cloud service facility,
ii. Access to the audit trail, and
iii. the internal control environment of the cloud service provider.

3. Manage identities, people and roles
Employees from the cloud service provider will inevitably have access to your firm’s applications and data. The employees at your organization that carry out operations on the provider’s system will also have access to this data.
A firm must ensure that the cloud service provider has sufficient policies to govern who has access to sensitive data and software. The cloud service provider must give the customer the privilege to manage and assign authorization for the users. They must also ensure their system is secure enough to handle different types of attacks on client data.

4. Enforcing privacy policies

Privacy and protection of personal and sensitive information are crucial to any organization's success. Personal data held by an organization could face bugs or security negligence. If a provider is not offering adequate security measures, the firm should consider seeking a different cloud service provider or not uploading sensitive information on the cloud.

5. Assess security vulnerabilities for cloud applications

Organizations have different types of data that they store in the cloud. Different considerations should be made according to the kind of data the firm intends to secure. Cloud application security poses diverse challenges to both the provider and the firm. Depending on the deployment model of the cloud service provider e.g., IaaS, SaaS, or PaaS, there are different considerations for both parties.

6. Cloud networks security

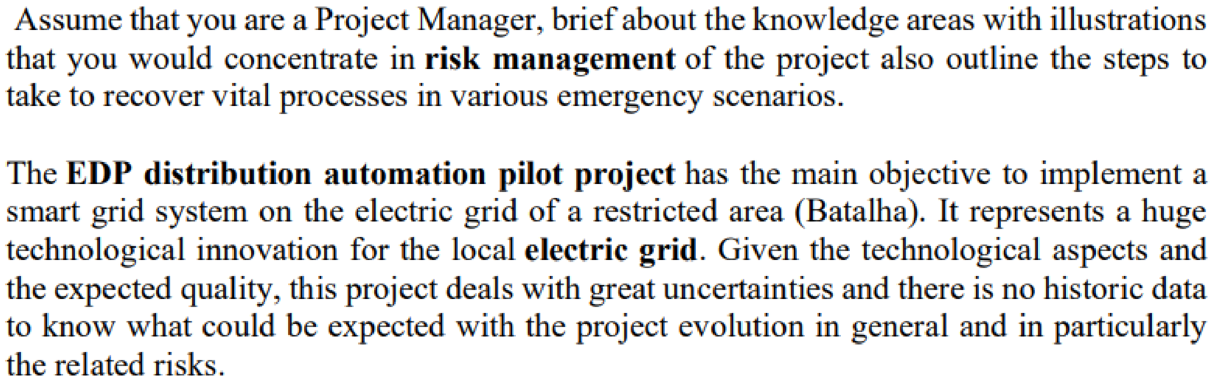
Audits of the cloud networks should be able to establish malicious traffic that can be detected and blocked. However, the cloud service providers have no way of knowing which network traffic its users plan to send or receive. Organizations must then work together with their service providers to establish safety measures.

7. Evaluating physical infrastructure and security controls

The security of the physical infrastructure of an IT system determines its vulnerability at the onset of a malicious attack. The provider must assure its users that appropriate measures are in place. Facilities and infrastructure should be stored in secure locations and backed up to protect against external threats.

It is becoming more critical to maintain privacy and security with more data and software being migrated to the cloud. The IT groups must consider the cloud security risks and implement solutions to ensure the security of client data stored and processed in the cloud.

3.



Assume that you are a Project Manager, brief about the knowledge areas with illustrations that you would concentrate in **risk management** of the project also outline the steps to take to recover vital processes in various emergency scenarios.

The **EDP distribution automation pilot project** has the main objective to implement a smart grid system on the electric grid of a restricted area (Batalha). It represents a huge technological innovation for the local **electric grid**. Given the technological aspects and the expected quality, this project deals with great uncertainties and there is no historic data to know what could be expected with the project evolution in general and in particularly the related risks.

The four important processes for risk management would be:

1. frame risk

2. assess risk

3. respond to risk once determined

4. monitor the risk

Risk Frame:

Establishing a realistic and credible risk frames which are identified by the organization themselves.

1.1 like assumption about the threats, vulnerabilities and likelihood of occurrence the affect how risk is assessed

1.2 Priorities and trade-off the organizations have and can afford. Trade-off among different

types of risk that organization face, time frames in which org must address risk

the risk framing component and the associated risk management strategy also include any strategic level decision on how risk to prg operations and assets, individuals, other org.

Risk Assessment:

purpose of risk assessment component is:

2.1 threats to org or threats directed through org against other org or the nation

2.2 vulnerabilities internal and external to org

2.3 the harm to org that may occur given the potential for threats exploiting vulnerabilities

2.4 the likelihood that harm may occur

Risk Response:

the purpose of risk response component is to provide a consistent, org-wide response to risk in accordance with the org risk frame:

3.1 developing alternatives courses of action for responding to risk

3.2 evaluating the alternative courses of action

3.3 determining appropriate courses of action consistent with organizational risk tolerance

3.4 implementing risk responses based on selected courses of action

Risk Monitoring:

Analysing monitoring results gives organizations the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed.

The results from the risk identification, qualitative and quantitative risk analysis, risk response planning and monitoring are summarized. Since the results of risk monitoring and control resulted from just one iteration, it is not possible to conclude about the result or impact of this methodology to the current pilot project.

- The project risk methodology is new for the project management team, so first should be assured that project team understands the project risk management plan and is committed to follow it.
- The project had already started when the risk management plan was defined, once the ideal timing for establishing the risk management plan is along with the project management plan, when the project is defined and characterized, so it is easily accepted along with the other project management practices.

In order to attain this important goal for EDP distribution, an action research project was required, which had established the following objectives:

- Design a risk management methodology adapted to the project characteristics, which includes the risk management planning, risk identification, risk qualitative and quantitative assessment, risk response planning and risk monitoring and control processes.
- Provide all the necessary templates for the risk management processes.
- Adapt the risk management methodology to future similar projects

Recovering data:

Step One: Create a list of all possible threats to the project
Threats come in all forms and sizes. As a first step towards data recovery after a disaster, a project organization should list all possible threats and categorize them according to the magnitude of impact those threats would inflict on the system if they materialized.
The project should also draw a clear picture of its system downtime tolerance based on how much time it can afford to be down without too big an impact on the overall well-being of the project.

Step Two: Outline the project continuity and data recovery infrastructure
A project' ability to respond to a disaster is only as good as its project continuity and disaster recovery (BCDR) infrastructure. This includes high speed/high bandwidth connections, main data centre, a resource duplication remote site and uninterrupted power supply. Failure to have this infrastructure in optimal performance automatically translates to serious obstacles to a project' profits once disaster strikes.

Step Three: Build a precise inventory of the project' IT assets
A precise inventory of the IT assets in a project draws a clear picture of the available project resources as well as the project processes to protect in the event of a disaster. A single disaster that strews a company's resources can recede every progress the project has ever made since inception

4. ANS

The four important process for risk management would be:

1. frame risk

2. assess risk

3. respond to risk once determined

4. monitor the risk

Risk Frame:

Establishing a realistic and credible risk frames which are identified by the organization themselves.

1.1 like assumption about the threats, vulnerabilities and likelihood of occurrence the affect how risk is assessed

1.2 Priorities and trade-off the organizations have and can afford. Trade-off among different

types of risk that organization face, time frames in which org must address risk

the risk framing component and the associated risk management strategy also include any strategic level decision on how risk to prg operations and assets, individuals, other org.

Risk Assessment:

purpose of risk assessment component is:

2.1 threats to org or threats directed through org against other org or the nation

2.2 vulnerabilities internal and external to org

2.3 the harm to org that may occur given the potential for threats exploiting vulnerabilities

2.4 the likelihood that harm may occur

Risk Response:

the purpose of risk response component is to provide a consistent, org-wide response to risk in accordance with the org risk frame:

3.1 developing alternatives courses of action for responding to risk

3.2 evaluating the alternative courses of action

3.3 determining appropriate courses of action consistent with organizational risk tolerance

3.4 implementing risk responses based on selected courses of action

Risk Monitoring:

Analysing monitoring results gives organizations the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed.

DATA RECOVERY PLAN:

1. Have a Data Backup and Recovery Plan

Responsibility for each stage of the data journey in the plan should be clear so managers and their team are aware of accountability. The formal detailed plan will also help with the onboarding of new employees.

2. Centralise the Data

It's important you keep backups of data in at least one safe place. This helps to reduce the chance of mismanagement and is more organised so if you ever do need to refer to the backups, they're easily retrieved.

Consider having a mixture of offsite (such as USB drives and tapes) and online backups to ensure that your data will be safe from harm

5. ANS:

The four important processes for risk management would be:

1. frame risk
2. assess risk
3. respond to risk once determined
4. monitor the risk

Risk Frame:

Establishing a realistic and credible risk frames which are identified by the organization themselves.

1.1 like assumption about the threats, vulnerabilities and likelihood of occurrence the affect how risk is assessed

1.2 Priorities and trade-off the organizations have and can afford. Trade-off among different

types of risk that organization face, time frames in which org must address risk

the risk framing component and the associated risk management strategy also include any strategic level decision on how risk to prg operations and assets, individuals, other org.

Risk Assessment:

purpose of risk assessment component is:

2.1 threats to org or threats directed through org against other org or the nation

2.2 vulnerabilities internal and external to org

2.3 the harm to org that may occur given the potential for threats exploiting vulnerabilities

2.4 the likelihood that harm may occur

Risk Response:

The purpose of risk response component is to provide a consistent, org-wide response to risk in accordance with the org risk frame:

3.1 developing alternatives courses of action for responding to risk

3.2 evaluating the alternative courses of action

3.3 determining appropriate courses of action consistent with organizational risk tolerance

3.4 implementing risk responses based on selected courses of action

Risk Monitoring:

Analysing monitoring results gives organizations the capability to maintain awareness of the risk being incurred, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed.

It is divided into 3 tiers

tier 1 : ongoing threat assessments
tier 2: analysis of new or current technologies or analysis of tech which company is considering to use in future

tier 3: focuses on information systems and includes automated monitoring of standard configuration settings for information tech product, vulnerability scanning and ongoing assessments of security controls.

DATA RECOVERY PLAN:

1. Have a Data Backup and Recovery Plan

Responsibility for each stage of the data journey in the plan should be clear so managers and their team are aware of accountability. The formal detailed plan will also help with the onboarding of new employees.

2. Centralise the Data

It's important you keep backups of data in at least one safe place. This helps to reduce the chance of mismanagement and is more organised so if you ever do need to refer to the backups, they're easily retrieved.

Consider having a mixture of offsite (such as USB drives and tapes) and online backups to ensure that your data will be safe from harm

3. Back up at Regular Intervals

Losing data, especially important business files, is the stuff of nightmares - particularly when you don't know at what point in time your data became corrupt or what it is that infected your work in the first place. The best business practice is to always back up your data.

Every business owner (or anyone, for that matter) knows how important this is but it's still too easy to think it will never happen to you. In the world of data recovery, it's not a matter of whether you experience data loss but when. Being ill prepared can lead to devastating consequences ranging from lost vital business data (which you may never be able to retrieve) and wasted productivity to damaged reputation and client impression, not to mention costing big bucks in repairs.

4. Maintain & Go Beyond Compliance

Huge international corporations such as PlayStation and Dropbox have been hit by hackers in the past. But because these companies are so big and their reputations were so strong, they managed to survive. Smaller businesses don't have the billions in capital to help weather the storm so it's even more imperative that they follow the right protocols when it comes to data protection.

It's even better if you try and go beyond the basic compliance practices.

5. Manage Access & Control

Ensure sensitive data stays well protected and secure by allowing only authorised team members access. Make sure you keep a note of who is allowed to add to or modify your data and its relevant backups in order to prevent any breaches.

6. Handle Devices with Care

Make sure that your backup devices are always handled with care. This doesn't mean just ensuring nobody drops their laptop (although that's also important and it's worth reminding Young Bilal every now and then). Ensure your authorised team members know how to modify the data when they need to and that they know the security risks involved and how to handle them.

In addition, as well as having physical backups, consider storing the information securely in a cloud-based system too.