Name : Yimsheungyat
Course: SRM-PCOM7E March2023

内容

Unit 2 User Participation in the Risk Management Process

Introduction of Qualitative and Quantitative assessment

Quantitative vs Qualitative Assessment

Qualitative risk assessment	Quantitative risk assessment

1. Analyze risk based on subjective assessment	1 Application of mathematical and systematic approach
2. Relied on identification of potential risk and assessment of likelihood based on qualitative factors severity, frequency and vulnerability	2 Quantify the potential consequences in terms of financial Financial loss, damage, impact
3. Involve structured analysis of risk	3 Evaluate and select mitigation strategies
4. Often used when there is limited data and uncertainty involved	4 Often used in re-evaluate the risk exposures and mitigation strategies
5. Commonly used in project	

The advantages of involving users in the risk management process

- Improved accuracy of risk identification
  Users are more knowledgeable about details and nuances
- Increased ownership and responsibility
  Users feel a sense of ownership and responsibility towards mitigating risks
- Better risk assessment and prioritization
  User can provide insights into potential impact to identifies risks
  Can help in assessment and prioritize risk
- Enhanced communication and collaboration
  Building consensus on the significance of identified risk

Questions to think

1. How will the lack of user access affect the risk assessment you will carry out as part of your assessment?
2. Will it affect the choice of Qualitative vs. Quantitative assessment methods you utilize?
3. How might you mitigate any issues encountered?

The lack of user assessment can significantly affect the risk assessment process; it can lead to faulty risk identification, inadequate risk assessment, and suboptimal risk mitigation strategies.

1. Incomplete risk identification
2. Inaccurate risk assessment

3. Inefficient risk mitigation
4. Inadequate risk communication

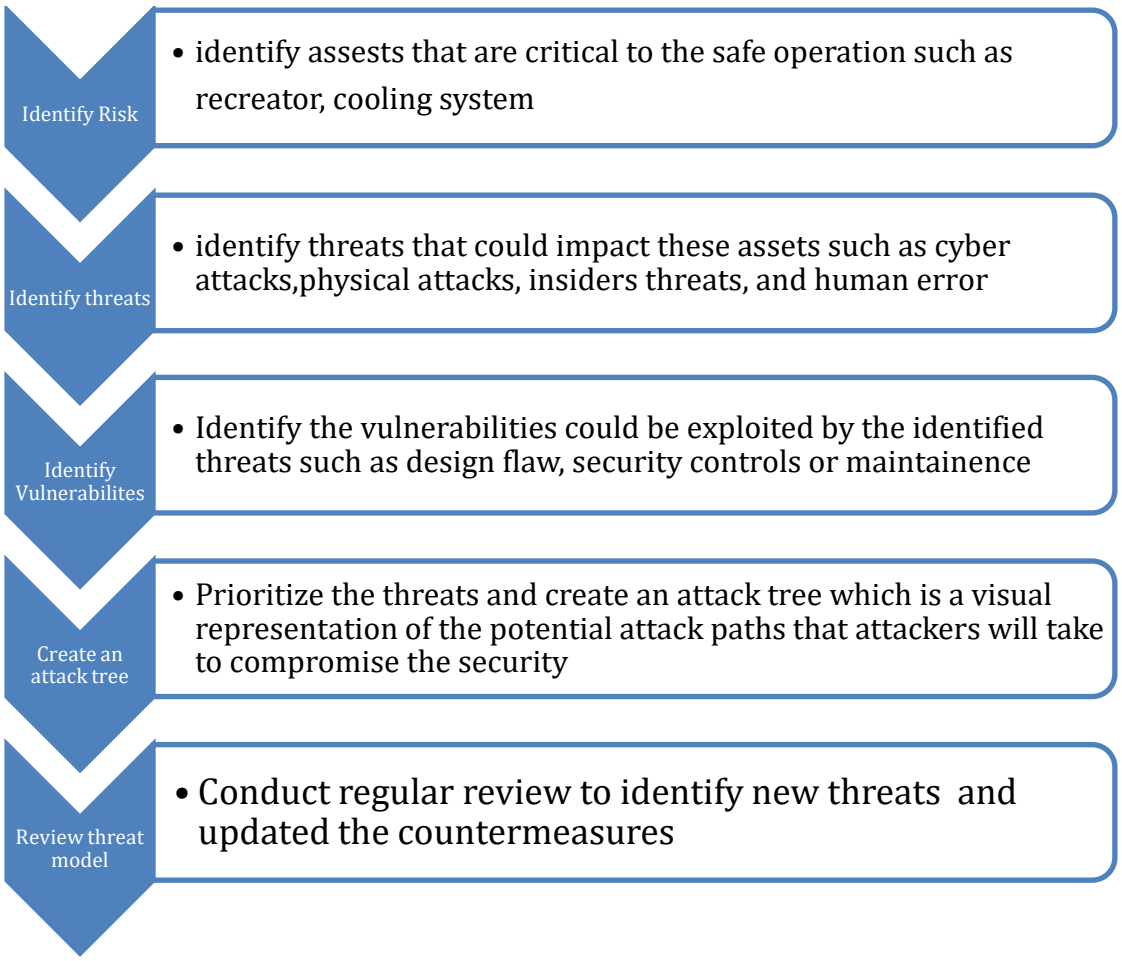
In essence, user assessment is critical to an effective risk assessment process. Without their input, the risk assessment process may miss important risks and may lead to inadequate or ineffective risk mitigation strategies and procedures.(advisera, 2022)

References

Advisera 2022 available at ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide (advisera.com)

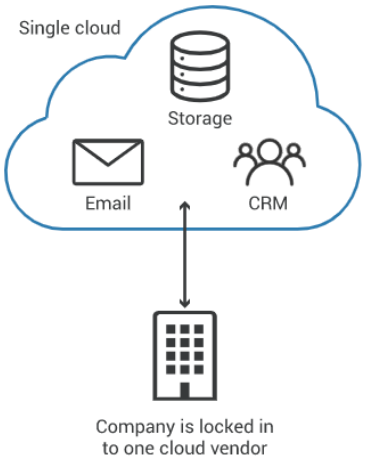
Unit 4 Threat Modelling Exercises

To prevent any disasters and catastrophic incidents occurred in our massive infrastructures that may lead to tremendous casualties, threat model such as STRIDE DREAD, and Open Web Application Security Project (OWASP) should be adopted. In response to scenarios of a large nuclear power station in France, a threat model is created as follows:



Unit 10 DR Solution Design and review

The vendor lock-in problem in cloud computing occurs when clients become reliant (i.e., locked-in) on a single cloud provider's technological implementation and are unable to switch vendors in the future without incurring significant fees, legal restrictions, or technical incompatibilities. (Cast AI 2023)



1. Limited Flexibility	Restricts organization to response quickly to change business needs due to difficulties to customize existing systems with other technologies
2. High Cost	Services provider lay high prices
3. Limited portability	difficult to migrate to another solution without incurring significant costs and potential data loss
4. Security Risk	exposes the organization to security risks as they may be vulnerable to attacks or data breaches that the vendor is unable or unwilling to fix

MITIGATION STRATEGIES

- **Multi-cloud or hybrid cloud strategy**
- **Backups**
- **Ensure data can be moved easily**
- **Evaluate cloud services carefully**

CLOUD COMPUTING

Modern cloud computing offers many benefits, including scalability, flexibility, and cost savings, but it also comes with significant security concerns. Here are some of the main security concerns with modern cloud computing:

1. Data breaches
2. Malware attacks
3. Insider threats
4. Misconfigured systems
5. Data loss
6. Lack of control

The mitigation methods are as follows:
1 choose cloud providers
2 implement strong access controls
3 authentication mechanisms
4 enforce strict data protection policies.
5 Regular audits and security testing should also be conducted to ensure that data and applications are secure.

References

Cast AI 2023 available at What Is Cloud Vendor Lock-In (And How To Break Free)? - CAST AI – Kubernetes Automation Platform