Research Methods and Professional Practice

DESIGN & IMPLEMENT CLOUD SECURITY (IAM/DATA SECURITY) FRAMEWORK AND DEVELOP CLOUD INCIDENT RESPONSE- RESEARCH PROPOSAL (UNIT-10)

AGENDA

- Project Requirements & Deliverables Mapping
- Research Questions & Contribution
- Aims and Objectives
- Key literature related to the project
- Methodology/Research Design
- Ethical considerations and risk assessment
- Description of artefact(s) that will be created (if applicable)
- Timeline of proposed activities

PROJECT REQUIREMENTS

- British Computer Society (BCS) criteria
  - Establish practical work using computing/IT technology
  - Define the research problem and establish its objectives
  - Final Report covering results, lessons learned etc.
- CyBOK Knowledge Area
- Required for MS-Cybersecurity

* References in the notes

DELIVERABLES MAPPING

REQUIREMENT	ARTEFACT
Problem understanding & existing research	Literature Review Research Development
Demo in knowledge application	Cloud Security Assessment for the research questions (IAM, Data Security, Incident Response)
Establish a technical skill through demonstration	
CyBok Knowledge Areas	Network Security Access Control Cryptography Security Operations and Incident Response

* References in the notes

How the project meets the MS requirement

REQUIREMENT	Mapping
Research Depth	Literature review and consequent framework design exhibit a comprehensive exploration of prior research, displaying the ability to assess and integrate material in a critical manner.
Core Concepts	The project explores essential ideas that are integral to the curriculum of the MS programme, including identity and access management, data security, and incident response.
Application of Methodologies	The project utilizes a combination of techniques, encompassing participatory design, practical implementation, and testing. This is consistent with the program's focus on the use of various research approaches.
Artifact Creation	The development of physical artefacts, such as the documentation for the Cloud Security Framework and the Incident Response system, is in accordance with the program's emphasis on practical and concrete results.

* References in the notes

RESEARCH QUESTIONS

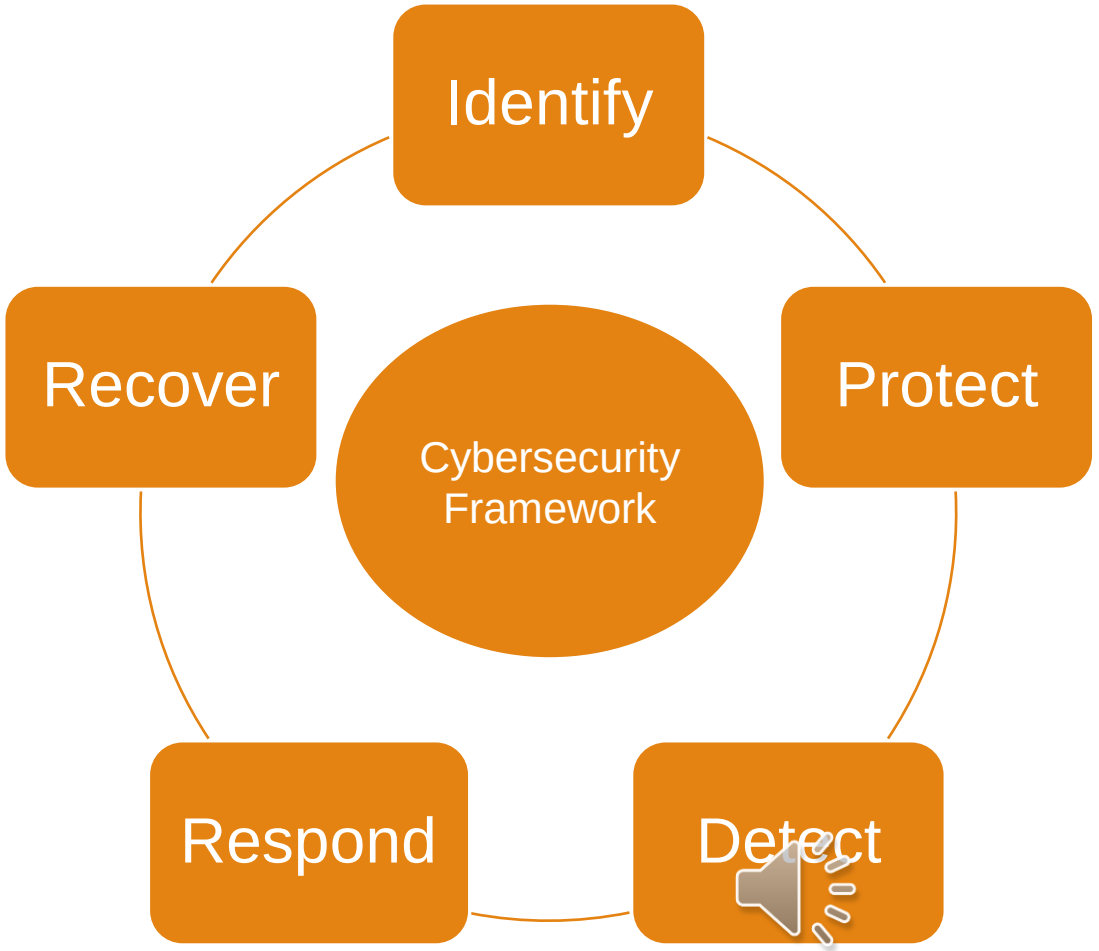
- How can organizations assess & implement identity and access management controls in cloud environments to prevent unauthorized access and privilege escalation?
- What are the best practices for data encryption in various cloud service categories (IaaS, PaaS, SaaS) implementation, and how can the efficacy of encryption measures be evaluated?
- How can the network security of cloud be evaluated, improved and implemented?
- How can organizations ensure a quick and coordinated response to security incidents? What are the key elements of an effective incident response plan tailored to cloud environments?

* References in the notes

RQ-1

(How can organizations assess & implement identity and access management controls in cloud environments to prevent unauthorized access and privilege escalation?)

- Thorough analysis of the current cloud infrastructure against NIST Cyber Security Framework (CSF)
- Identify any potential vulnerabilities or gaps in their access controls.
- Regular security audits and penetration testing to identify any weaknesses in the system.
- Clear understanding of the cloud service provider's security measures and protocols
- Proactively identify and address any vulnerabilities in their cloud infrastructure
- Helps to minimize the risk of unauthorized access or data breaches.
- Understanding and aligning with the security measures and protocols of the CSP
- Enhance their overall security posture and protect their sensitive data in the cloud.

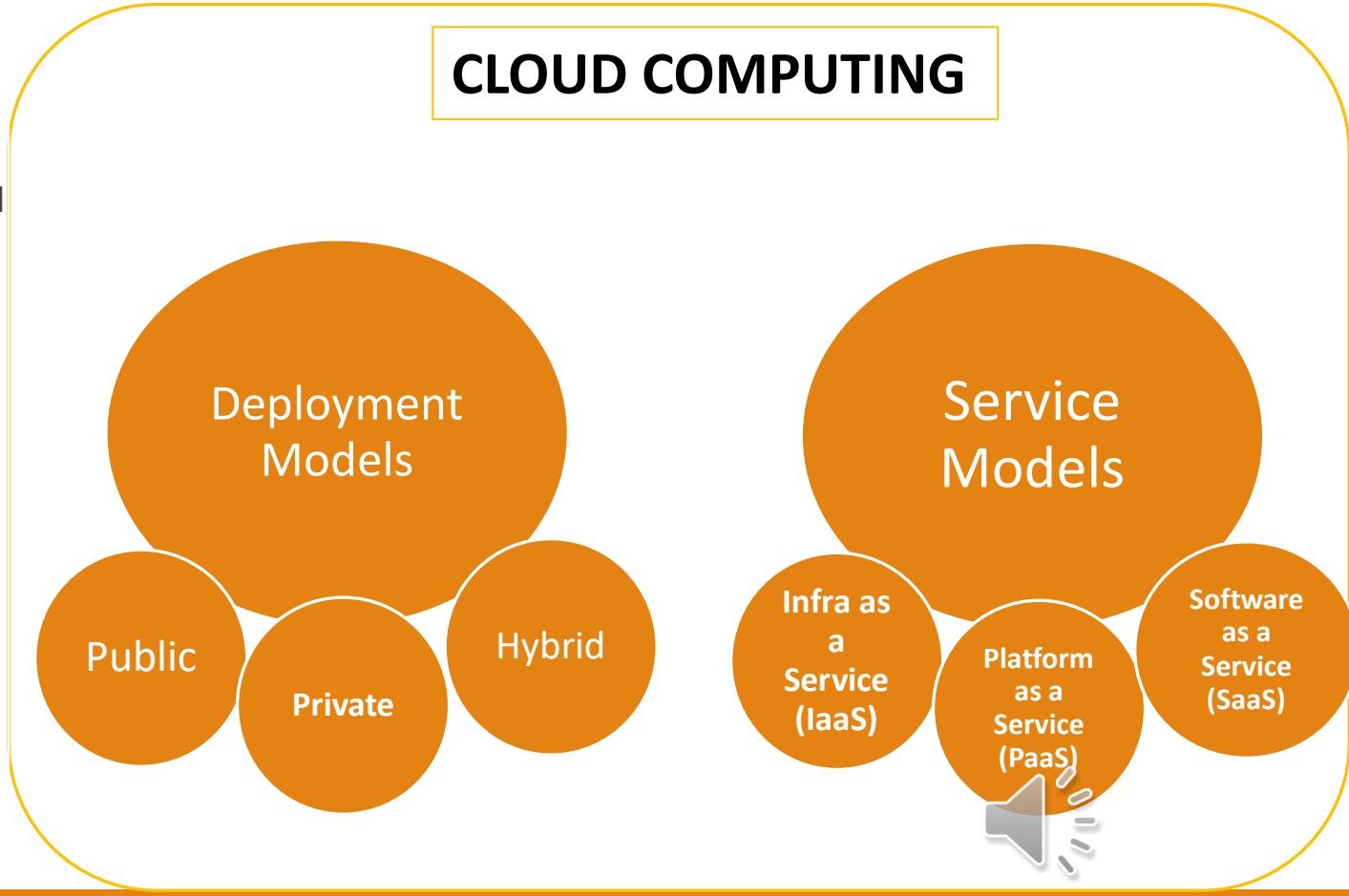


* References in the notes

RQ-2

(What are the best practices for data encryption in various cloud service categories (IaaS, PaaS, SaaS) implementation, and how can the efficacy of encryption measures be evaluated?)

- Best practices for data encryption in various cloud service categories include implementing encryption at all cloud stack layers, including data at rest, in transit, and in use.
- Infrastructure as a Service (IaaS): Encrypting VMs, backups and storage.
- Platform as a Service (PaaS): Encrypting application data, databases, and communication channels is critical.
- Software as a Service (SaaS): Ensure that the strong encryption for data storage and transmission is provided by the provider
- Regular audits, penetration testing, and vulnerability assessments can be used to evaluate the efficacy of encryption measures by identifying any weaknesses or vulnerabilities in the encryption deployment.



* References in the notes

RQ-3

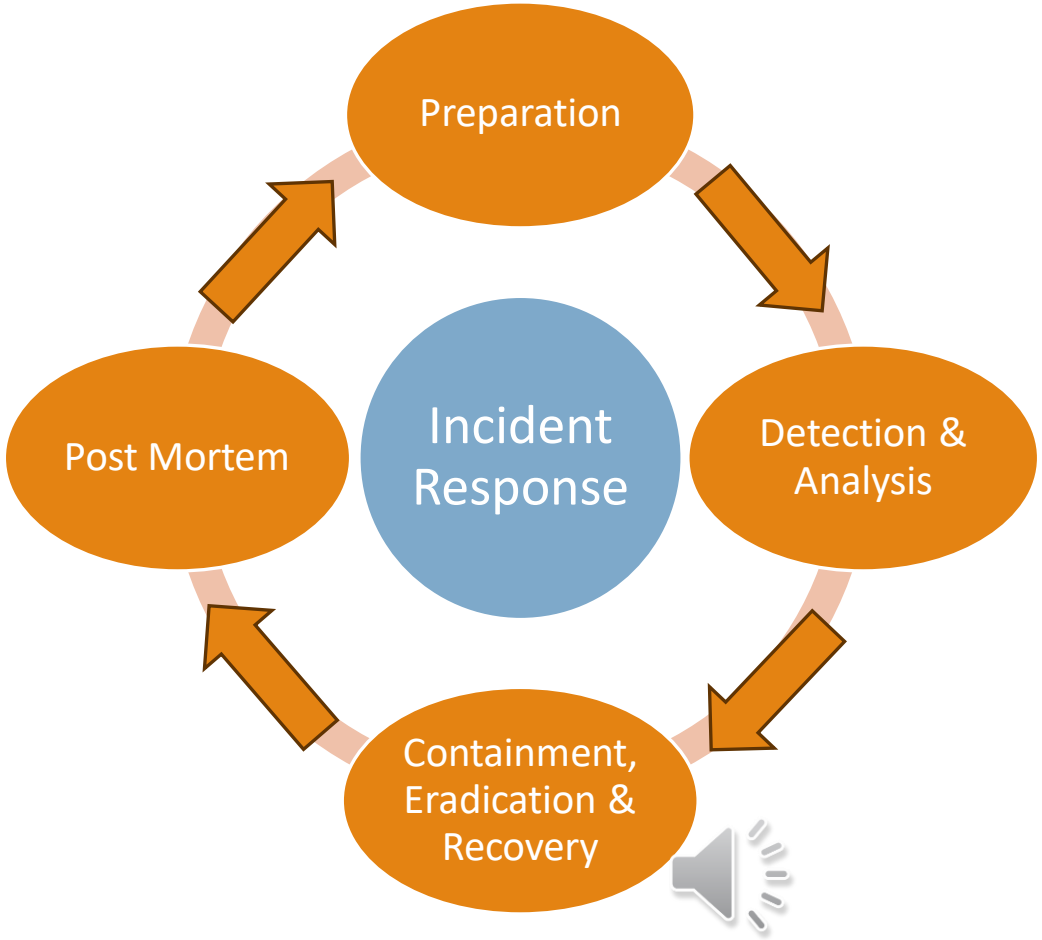
(How can the network security of cloud be evaluated, improved and implemented?)

- Conduct exhaustive risk assessments to identify potential hazards and weaknesses.
- Implementing robust authentication and access controls to ensure that only authorized users have access to sensitive data and resources.
- Monitoring and recording network activity on a regular basis should detect any suspicious or unauthorized access attempts.
- Implementing comprehensive security measures, such as firewalls (Security Groups, Network Access Control Lists), intrusion detection systems, and network segmentation, to enhance the network's overall security.
- Ensure that the cloud service provider has in place the appropriate security protocols and follows industry best practices to protect data during transmission and storage.

RQ-4

(How can organizations ensure a quick and coordinated response to security incidents? What are the key elements of an effective incident response plan tailored to cloud environments?)

- For quick and coordinated response , organizations should have a specific incident response plan for cloud environments
- A cloud-based incident response plan requires:
  - A designated incident response team,
  - Clearly defined roles and responsibilities,
  - Real-time monitoring and detection tools,
  - Incident escalation procedures, and
  - Regular evaluations and plan updates.
- By implementing these components, cloud security incidents can effectively be mitigated and responded to.



* References in the notes

AIMS & OBJECTIVES

- Develop & Deploy IAM and Data Security Measures and Develop Cloud Incident Response

OBJECTIVES:

- Develop a comprehensive cloud security framework for Identity and Access Management (IAM) and data security
- Encrypt data and implement access controls to ensure complete Data Security
  - To implement the framework in cloud environment
- Evaluate the effectiveness of Data Security & IAM measures
- Develop Cloud Incident Response

* References in the notes

Key Literature

Literature	Relevance
Cloud Security Alliance (CSA) Cloud Security Guidance and Cloud Controls Matrix	CCM is comprehensive cloud security control framework – designed to assess & manage the cloud security risks.
Cloud Security Posture Management (CSPM)	CSPM tools use the information from different sources (like NIST, CIS etc.) to assess and improve the cloud security posture.
National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)	NIST CSF is a framework that provides a common language and methodology to manage cybersecurity risk – used by businesses of all sizes to enhance the cybersecurity posture.
NIST SP 800-61 Computer Security Incident Handling Guide	Exhaustive guide to managing computer security incidents-step-by-step approach for responding effectively to security incidents.
CIS Benchmarks	CIS Benchmarks are a collection of configuration standards designed to enhance an organization's security posture by minimizing the attack surface.
White papers and technical reports from cloud providers	To understand the cloud provider (AWS /Azure /GCP) related configurations & controls

* References in the notes

Methodology / Research Design

- Literature review to understand the existing best practices, frameworks related to IAM/Data Security & IR in cloud environ

- Framework should be designed iteratively, taking into account industry standards, regulatory needs, and the specific attributes of the organization's cloud infrastructure - ensures that the framework is aligned with organizational goals .

- The implementation of Identity and Access Management (IAM) and Data Security safeguards is necessary. It is advisable to conduct testing of the configurations in a controlled environment prior to deployment.

- Utilize a threat modelling methodology for determining potential security events and thereafter devise an Incident Response framework in alignment with the identified threats.

- Perform an assessment of IAM and Data Security setups. Document the whole process undertaken, as well as present the findings and recommendations.

- The Cloud Security Framework should be enhanced by incorporating insights gained from past experiences and taking into account the evolving landscape of security threats.

* References in the notes

ETHICAL CONSIDERATIONS & RISK ASSESSMENT

- Ensure that any data used for testing or simulations has been anonymized and is obtained with the appropriate permissions.
- When handling sensitive data, adhere to applicable data protection regulations and guidelines
- A risk assessment will be undertaken to identify potential dangers associated with the research endeavor. Adequate mitigation strategies will be implemented to effectively manage and mitigate any identified risks.

* References in the notes

Artefacts

Following Artefacts will be created:

- **Documentation of Cloud Security Framework**
  - Comprehensive documentation providing a thorough explanation of the design, execution, testing and setup of the Identity and Access Management (IAM) as well as Data Security procedures.
- **Cloud Incident Response System**
  - Documentation and implementation of the integrated Cloud Incident Response system.

* References in the notes

PROJECT TIMELINES

Task	Assigned To	% Allocation	Status	Start Date	End Date	Duration	Predecessors	At Risk
Cloud Assessment & Implementation				11/06/23	04/19/24	120d		
Literature Review	Amit p	100%	Not Started	11/06/23	12/29/23	40d		
Define Scope and Objectives	Amit p	100%	Not Started	11/06/23	11/17/23	10d		
Identify and Collect Relevant Literature	Amit p	100%	Not Started	11/20/23	12/01/23	10d	3	
Analyze and Summarize Literature		100%	Not Started	12/04/23	12/15/23	10d	4	
Identify Gaps		100%	Not Started	12/18/23	12/29/23	10d	5	
Framework Design and Implementation	Amit p	100%	Not Started	01/01/24	02/23/24	40d	2	
Meetings and Collaboration	Amit p	100%	Not Started	01/01/24	01/12/24	10d		
Framework Design	Amit p	100%	Not Started	01/15/24	01/26/24	10d	8	
IAM and Data Security Implementation	Amit p	100%	Not Started	01/29/24	02/09/24	10d	9	
Testing, Feedback and Refinement		100%	Not Started	02/12/24	02/23/24	10d	10	
Incident Response System Integration	Amit p	100%	Not Started	02/26/24	03/22/24	20d	7	
Threat Modelling & Design	Amit p	100%	Not Started	02/26/24	03/08/24	10d		
Implement the IR system	Amit p	100%	Not Started	03/11/24	03/22/24	10d	13	
Testing, Evaluation, and Documentation	Amit p	100%	Not Started	03/25/24	04/19/24	20d	12	
Testing Configurations (IAM/Data Security)	Amit p	100%	Not Started	03/25/24	04/05/24	10d		
Analyze results & Document	Amit p	100%	Not Started	04/08/24	04/19/24	10d	16	

- Duration – 6 months
- Actual dates will vary based on the start date
- Risk Legends

Low

Medium

High

* References in the notes

References

- Rashid, A., Chivers, H., Danezis, G., Lupu, E. & Martin, A. (2021) CyBOK: Cyber Security Body of Knowledge. 2nd ed. United Kingdom: The National Cyber Security Centre Available from: https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf> [Accessed 04 October 2023]
- BCS. (2022) Academic Accreditation guidelines. https://www.my-course.co.uk/pluginfile.php/1003183/mod_resource/content/1/BCS%20Project%20Requirements.pdf [Accessed 05 October 2023]
- Erukalla, R., Nachmany, A., Gupta,R.,Kulkarni,S. (2023) What is IAM For the Cloud. Available from: https://cloudsecurityalliance.org/artifacts/what-is-iam-for-the-cloud/ [Accessed 06 October 2023]
- Luttrell,M., Joy,J. (2022). IAM policy types: How and when to use them. Available from: https://aws.amazon.com/blogs/security/iam-policy-types-how-and-when-to-use-them/?secd_iam8 [Accessed 08 October 2023]

References

- Beer,K. (2020) The importance of encryption and how AWS can help. Available from: https://aws.amazon.com/blogs/security/importance-of-encryption-and-how-aws-can-help/ [Accessed 07 October 2023]
- Cichonski,P., Millar, T., Grance, T., Scarfone, K. (N.D.). Computer Security Incident Handling Guide.Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [Accessed 08 October 2023].
- National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. https://doi.org/10.6028/NIST.CSWP.29.ipd
- Mogull,R., Arlen, J., Gilbert, F., Lane,A., Mortman,D., Peterson,G., Rothman,M. (2017). Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. Available from: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/#related_resources [Accessed 08 October 2023].

References

- Cloud Controls Matrix v3.0.1 (2021). Available from: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/ [Accessed 10 October 2023].
- CIS Benchmarks (N.D). Available from: https://downloads.cisecurity.org/#/ [Accessed 10 October 2023].
  - CIS Amazon Web Services Foundations Benchmark
  - CIS Microsoft Azure Foundations Benchmark
- Wiz Experts Team(2023). CSPM explained . Available from: https://www.wiz.io/academy/what-is-cloud-security-posture-management-cspm [Accessed 11 October 2023].
- What is CSPM (N.D.). Available from: https://www.microsoft.com/en-us/security/business/security-101/what-is-cspm [Accessed 12 October 2023].


THANK YOU