# **SPECIAL OFFER –** CLOUD SECURITY ASSESSMENT

AWS

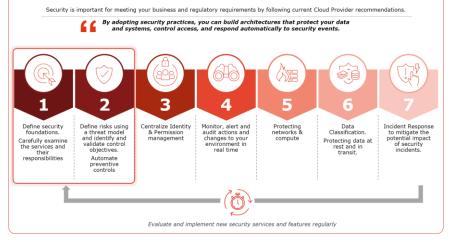
Governance

IAM

Cloud Security framework -

**ELCA** 

ELCACIoudServices



Security is important for meeting your business and regulatory requirements and to build secured architectures that protect systems and data, control access, and respond automatically to security events.

Following Cloud Well Architected principles, and Security Reference Architecture we will initiate within your organization the foundational mission scope to keep secure your systems and data along the time.

	Def	ine Corpora	te security p	olicy	
- Define t docume prioritie classific - Identify	ess priorities pusiness requirements nting business s and define a data ation. and priorities risks threat model.	Co reg de be	empliances & Policies llecting compliances and julatory constraints and fine corporate policies to applied to workload vironments.	•••••• •••••• ••••• ••••• ••••• ••••• ••••	Processes efine security processe d control objectives to fiely operate workloads efine review process to seep up to date security reat model.
1	2 2 4 4 4 4 4 4 4 5 4 5 4 5 4 5 4 5 4 5	- 6 areas o	f concerns	5 Protocian	6
Carefully examine the services you choose as your responsibilities vary depending on the services used, the integration of those services into your IT environment, applicable laws and regulations.	Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources.	Monitor, alert, and audit actions and changes to your environment in real time. Integrate log and metric collection with systems to automatically investigate and take action.	Automated software- based security mechanisms improve your ability to securely scale more rapidly and cost-effectively. Create secure architectures, including the implementation of controls that are defined and managed as code	Define a data classification that provides a way to categorize data based on levels of sensitivity, and encryption protects data by way of rendering it unintelligible to unauthorized access.	Implement mechanis to respond to and mitigate the potentia impact of security incidents. Your preparation strongly affects the ability of teams to operate effectively during an incident.

## Approach – Cloud Security & Risk –

( '' ک Initiate	Understand your context and risks	Define governance policies	Outline policy processes, SOC	Finalize
<ul> <li>Alignment on mission objectives, key questions, approach and organization</li> <li>Establish a basic understanding of the methodology</li> </ul>	What are your business and enternets?     Inserved tearthed your business risks as it relates to cloud?     What are your business priorities and trade-offs?     How do you annage the threats and data governance?     How do you audit for compliance?     What are the current teams, processies, skills to address security practices?	Establish controls objectives to ensure proper security of workloads     Establish policies to protect your network, assets and deta     Establish the operational management (environment, application or workload)     Establish policies to govern asset deployments and incidents     Establish IAM policies	Document SOC     Teams, Roles, Roles, Roles, Responsibilities	Presentation of the final reports     Exit strategy report     CCoE initial document     Plan the statement of works for implementation
	Initiate governance document listing your organization business risks, required components	Documented corporate policy statements and design guidance	List Governance process Define Governance MVP Define initial SOC	Final presentation and reports

Our proposed approach is divided into phases which allows to share intermediate results with your core team.

## **OBJECTIVES**

Your organization has started moved to the Cloud and wants to verify its security posture before a security accident happens.

Security

The mission outcomes is focused on the analysis of your security foundations, detection capability, and incident response to mitigate impact on your customers by security threat.

A remediation roadmap is proposed based on the security assessment outcomes.

#### **APPROACH** -

#### **Based on five disciplines:**

- 1. Security, Risk mitigation
- 2. Identity Management (IAM)
- 3. Infrastructure protection
- 4. Data Protection
- 5. Incident response

### RESULTS

- Security posture and remediation roadmap
- Roles, Responsibilities and Competencies
- Security architecture and review process

**ELCAC**loudServices

https://www.elcacloudservices.ch

 Exception, Revision, Communication process