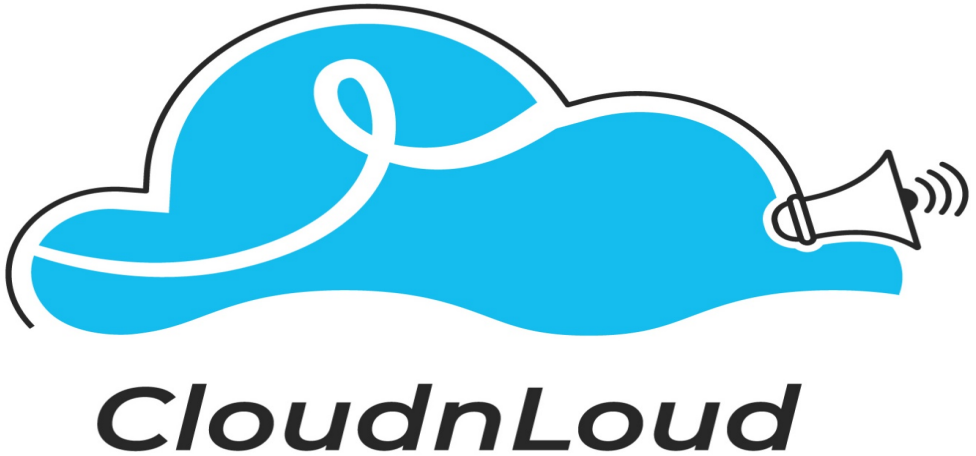
Security Assessment Overview



Not Just Skill Training

Enabling environment and scope to grow career

Security Assessment - Overview

- We must regularly test all controls to ensure that we protect or safeguard sensitive data / information.
- It’s a detailed review of the security of a system, application, or other tested environment.
- A trained information security professional performs a risk assessment that identifies vulnerabilities in the tested environment that may allow a compromise and makes recommendations for remediation, as needed.
- It’s normally an assessment report addressed to management that contains the results of the assessment in nontechnical language and concludes with specific recommendations for improving the security of the tested environment.

Security Assessment - Detailed Review

Business Need: Assess the requirement and plan according to business need

Risk Questions: Analyse existing architecture and raise relevant questions

Document: Document your updates on spreadsheet template

Industry: Design according to Industry standard

Regulations: Follow the Industry, Country and Regional Privacy law and prepare your solution accordingly.

HIPAA: The **Health Insurance Portability and Accountability** Act : It's process that business associates and covered entities follow to protect and secure Protected Health Information (PHI) as prescribed by the Health Insurance Portability and Accountability Act.

GDPR: EU law on **data protection and privacy in the European Union** and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

PIPEDA - The **Personal Information Protection** and Electronic Documents Act is a Canadian law relating to data privacy
GLBA - The Gramm–Leach–Bliley Act, also known as the **Financial Services Modernization**
SOX - The Sarbanes–Oxley Act, also known as the "Public Company Accounting Reform and **Investor Protection Act**"
PCI-DSS - The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes.

Security Assessment Template

Plan a template with current Risk, Detailed description of risk and Mitigation Recommendation

Assign values for each item (High / Medium / Low) based on Likelihood, Consequence and Risk Rating

Finally derive the **overall rating and decide**.

Simple Formula:
Risk = Impact * Likelihood

Most commonly used frameworks;

- NIST Risk Management Framework
- ISO 31000 series
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) Risk Management Framework
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) and the Security Risk

NIST Framework

A set of criteria that dictate how the United States government IT systems must be architected, secured, and monitored

It has six steps:

- **Step 1:** Categorize the system and the information that is processed, stored and transmitted by the system.
- **Step 2:** Select an initial set of baseline security controls for the system based on the categorization, tailoring and supplementing as needed.
- **Step 3:** Implement the security controls and document how they are deployed.
- **Step 4:** Assess the security controls to determine the extent to which they are meeting the security requirements for the system.
- **Step 5:** Authorize system operation based upon a determination that the level of risk is acceptable.
- **Step 6:** Monitor and assess selected security controls in the system on an ongoing basis and reporting the security state of the system to appropriate organizational officials.

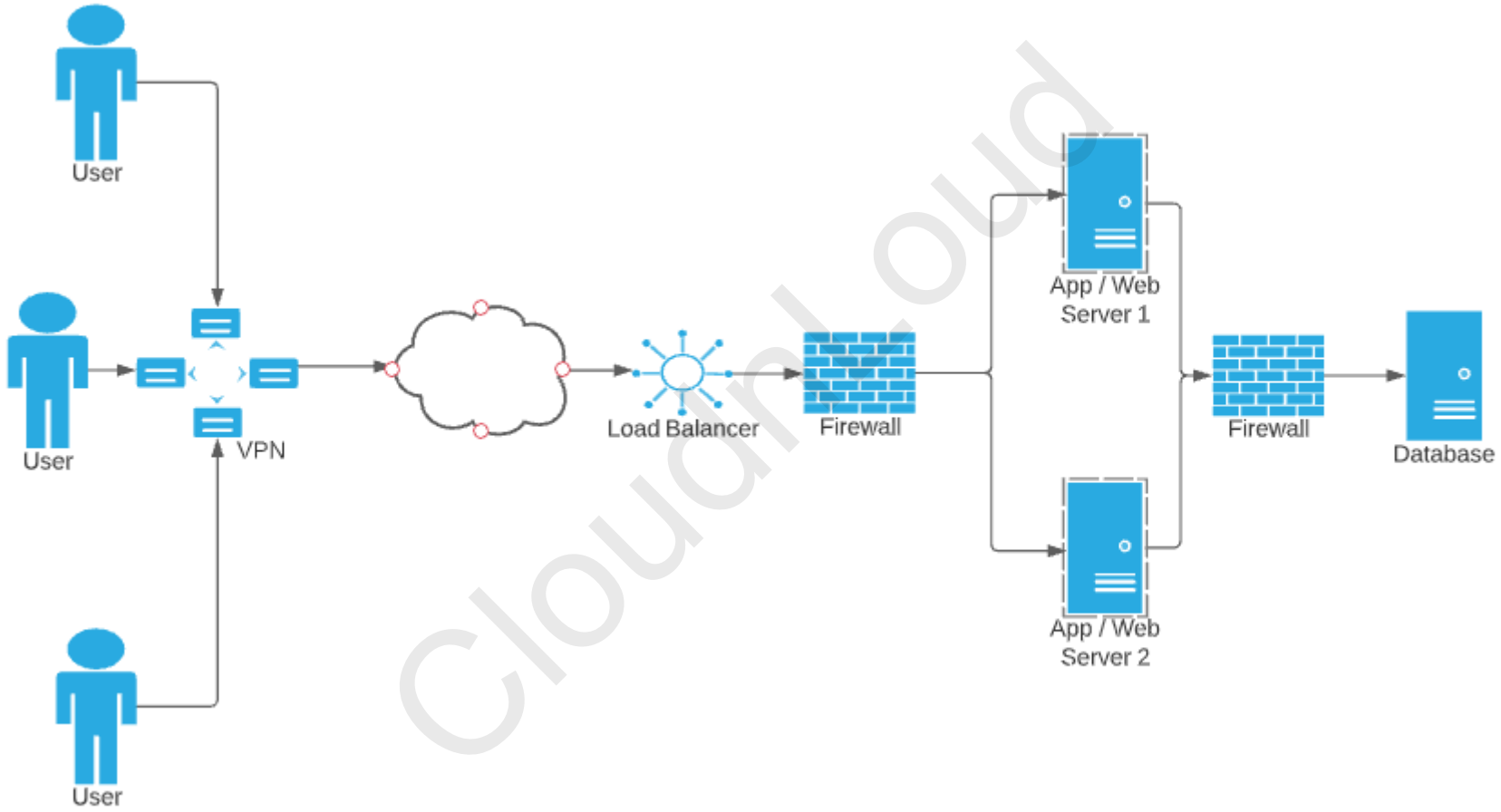
If we implement a risk assessment and governance strategy effectively by using RMF, it gives you plenty of operational benefits.

By using RMF in your organization, you will be automatically compliant.

Risk Assessment: Quantitative (Monetary benefits, and it takes time) &

Qualitative (Quickly prioritize and analysis like Critical, High, Medium and Low)

Security Assessment – Use Case 1



Key Terms - 1

- CIA
- GRC

Governance:

Governance is corporate management, Strategy, Policy management. Address Strategic planning, Business/IT Alignment, Policy creation and Vision Setting

Risk Management:

"Identifying risks, evaluating risks, and managing the risks.
Addresses System Threats, System vulnerability, Protection of IT Assets, and Risks to Management objectives"

Compliance:

Measure to ensure guarantee and conformity with laws, policies and formalities addresses adherence of a laws, regulations, policies and standards, best practices and frameworks

- Key Performance Indicators (KPI) - Backward looking metrics
- Key Risk Indicators (KRI) - Forward looking metrics

Categories of Risk

- Strategic.
- Operational.
- Financial.
- People.
- Regulatory.
- Governance.

Key Terms - 2

Risk Treatment:

- **Mitigate**
- **Accept**
- **Avoid**
- **Transfer**

Identifying Threats: Attackers, Assets, Software

- **Attackers**
- **Assets**
- **Software**

Categories of Risk:

- Strategic.
- Operational.
- Financial.
- People.
- Regulatory.
- Governance.

TIP of the Day

- Learn this tool in Public Cloud

- https://github.com/cyberark/SkyArk

- AzureStealth - Scans Azure environments

- AWStealth - Scan AWS environments