CloudAssure – AWS Security & Compliance Readiness Guide

Guidance Based on AWS Best Practices

Focus Areas

Focus	Details
Identity & Access Management	Root account security, MFA, least privilege
Detection & Monitoring	GuardDuty, Security Hub, CloudTrail, alerts
Data Protection	Encryption, KMS policies, secrets management
Network Security	VPC security, WAF/Shield
Incident Response	Playbooks, automation, simulations
Compliance Mapping	GDPR, NIS2, SOC2 alignment

Learning Outcomes

- Understanding of AWS Security Pillar key recommendations
- Checklist for risk reduction and compliance alignment
- Visibility into misconfigurations and risks
- Framework for building a security improvement roadmap

Example Improvements

Area	Typical Improvement
Critical Findings	50%+ reduction
MFA & Encryption Coverage	Move towards 100% enforcement
Compliance Readiness	+20–30% improvement

References

AWS Well-Architected Framework: https://aws.amazon.com/architecture/well-architected/

AWS Security Hub: https://aws.amazon.com/security-hub/

AWS GuardDuty: https://aws.amazon.com/guardduty/

AWS IAM Documentation: https://docs.aws.amazon.com/iam/

AWS Compliance Programs: https://aws.amazon.com/compliance/programs/