Cloud Security Misconfigurations and Compliance: An Empirical Model for DORA Readiness in Financial Environments

Ali Ferzali, Naol Mengistu, Elias Seid, Fredrik Blix (elias.seid@dsv.su.se)

Department of Computer and Systems Sciences

Stockholm University, Sweden

IARIA

Stockholm University

Agenda

- Introduction & Motivation
- Problem Statement andResearch Gap
- Research Question & Objectives
- Methodology
  - Research Strategy and Tool
  - Controlled Experiment Setup
  - Data Collection & Analysis
- Results and Interpretation
- Discussion
  - Answering the Research Question
  - Unique Contributions
  - Addressing Literature Gaps
- Conclusion and Future Work
- Q&A

Introduction & Motivation

- Rapid cloud adoption in financial services (scalability, cost-efficiency).
- Introduces new security challenges: Misconfigurations are a leading cause of breaches.
- Impact: Data exposure, compliance gaps, operational disruptions.

Introduction & Motivation

- EU's Digital Operational Resilience Act (DORA) – full effect in January 2025.
- Mandates robust ICT risk management for financial institutions.
- Focus on: Continuous monitoring, third-party (cloud provider) risk, operational resilience.
- Compliance is critical for operational integrity and avoiding penalties.

Research Problem

- Financial institutions struggle to align dynamic cloud security practices with DORA's stringent requirements.
- Traditional assessments (manual audits, periodic checks) are often insufficient for dynamic cloud environments.
- Lack of practical, automated tools that specifically map technical cloud misconfigurations to DORA articles.
- This leaves institutions vulnerable and potentially non-compliant.

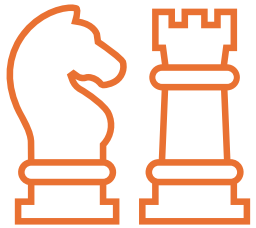
Research Gap

- Existing research often theoretical or focuses on general cloud security, not DORA-specific empirical validation.
- Limited experimental studies assessing AWS misconfigurations and their DORA implications.
- Need for data-driven models that bridge technical findings with regulatory mandates.

Research Question & Objectives

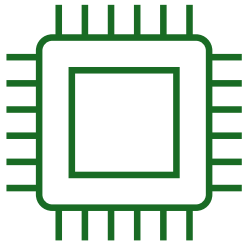
- **Research Question:** "How can an experimental security scanning model be utilized to identify common AWS misconfigurations and report their alignment with DORA compliance requirements?"
- **Objectives:**
  1. Identify common AWS cloud security misconfigurations.
  2. Develop and utilize a Python-based scanning script to conduct an empirical security assessment in a controlled AWS environment.
  3. Map identified misconfigurations to relevant DORA compliance requirements and provide actionable remediation insights.

Methodology - Research Strategy & Tool



Strategy: Experimental Research

Why? Empirical, data-driven, direct interaction with cloud, measurable insights.



Tool: Custom Python-based AWS Security Scanner

Utilizes AWS Boto3 SDK.

Focus on key AWS services: S3, EC2, IAM, VPC.

Designed for programmatic detection and DORA mapping.

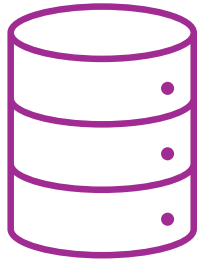
Methodology - Controlled Experiment Set-Up

- Controlled AWS Test Environment:
  - Intentionally introduced common misconfigurations (identified from literature).
    - S3: Public access, no encryption/logging.
    - EC2: Unrestricted SSH/RDP access.
    - IAM: Overly permissive roles, no MFA.
    - VPC: Default route to Internet Gateway, permissive ACLs, no Flow Logs.
  - Ensured a realistic testbed for scanner validation.

Methodology - Data Collection, Analysis & Reporting

- Data Collection: Scanner programmatically retrieves configuration data via Boto3.
- Data Analysis:
  - Rule-based: Checks against predefined security best practices & DORA-implied rules.
  - DORA Mapping: Misconfigurations automatically mapped to DORA Articles 5, 9, and 10.
- Reporting:
  - JSON output.
  - Interactive Streamlit Dashboard (Figure A.1 from Appendix could be shown here).
  - PDF Compliance Report.
- Source code: available on github.

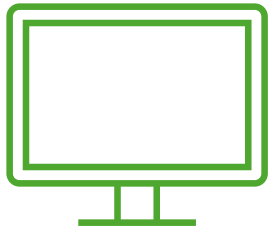
Results - S3 & EC2 Misconfigurations



S3 Compliance Issues:

- Public Access Enabled -> Mapped to DORA Art. 9 (Secure Configs). Rec: Enable all Public Access Block settings.

- Bucket Logging Disabled -> Mapped to DORA Art. 10 (Monitoring). Rec: Enable bucket logging.



EC2 Security Group Issues:

- Unrestricted SSH/ICMP/RDP Access (0.0.0.0/0) -> Mapped to DORA Art. 9. Rec: Restrict to known IPs, use VPN.

Results - IAM & VPC Misconfigurations

IAM Issues:

- Wildcard Permissions in Roles -> Mapped to DORA Art. 5 (ICT Risk Mgmt). Rec: Review, apply least privilege.

- MFA Not Enabled for Users -> Mapped to DORA Art. 5. Rec: Enable MFA.

- Inactive Privileged Accounts -> Mapped to DORA Art. 5. Rec: Review and deactivate.

VPC Issues:

- Default Route to Internet Gateway -> Mapped to DORA Art. 9. Rec: Verify intent, consider NAT Gateway for private subnets.

- Overly Permissive Network ACLs -> Mapped to DORA Art. 9. Rec: Restrict traffic.

- VPC Flow Logs Disabled -> Mapped to DORA Art. 10. Rec: Enable Flow Logs.

Interpretation of Findings

- High prevalence of misconfigurations confirms real-world challenges.
- Systemic risks emerge from default settings, lack of oversight, human error.
- Direct Impact on DORA Compliance:
  - Public S3/EC2 ports: Breaches Art. 9 (Secure Configs).
  - Weak IAM (no MFA, excessive perms): Breaches Art. 5 (Risk Mgmt).
  - Lack of logging (S3, VPC): Breaches Art. 10 (Monitoring, Governance).
- Scanner successfully bridges technical findings with specific regulatory requirements.

Discussion - Answering the Research Question

- **RQ:** "How can an experimental security scanning model be utilized to identify common AWS misconfigurations and report their alignment with DORA compliance requirements?"
- **Answer:**
  - The developed model *successfully identified* common AWS misconfigurations in a controlled setting.
  - It *effectively reported their alignment* by mapping each finding to relevant DORA Articles.
  - The model provides actionable insights, helping to proactively address compliance gaps.
  - Thus, an experimental model *can indeed* be effectively utilized for this purpose.

Discussion - Unique Contributions

- **Novel DORA-Focused AWS Security Scanner:** Open-source tool with integrated DORA compliance mapping for key AWS services.
- **Empirical Validation in a Controlled Environment:** Moves beyond theory to provide concrete evidence of misconfiguration impact on DORA compliance.
- **Bridging the Technical-Regulatory Divide:** Systematically connects technical AWS configurations to specific DORA articles, offering an adaptable experimental model.
- **Actionable Insights for Financial Institutions:** Provides practical means to identify pitfalls and strengthen operational resilience.

Discussion - Addressing Literature Gaps

- Fills the gap for *empirical, DORA-specific* assessment model.
- Provides a *practical, repeatable model* for linking technical AWS vulnerabilities to financial regulations like DORA, which was lacking.

Conclusion

- Successfully developed and evaluated an experimental model (AWS Security Scanner).
- Demonstrated capability to detect critical AWS vulnerabilities and map them to DORA Articles.
- Highlights direct regulatory implications of technical misconfigurations.
- Contributes a novel, DORA-focused open-source tool and an integrated technical-regulatory mapping model.
- Underscores the necessity of compliance-aware security tools for financial institutions under DORA.

Future Directions

- **Multi-Cloud Support:** Extend to Azure, Google Cloud.
- **Expanded DORA Compliance:** Cover more DORA mandates.
- **Support for Additional Frameworks:** GDPR, PCI-DSS.
- **Support for Additional Cloud Services.**
- **AI-Driven Remediation:** More sophisticated, context-aware recommendations.
- **Full Automation:** Continuous monitoring and automated remediation.
- **Real-World Validation:** Case studies in production environments.

Thank You!