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

Ali Ferzali, Naol Mengistu, Elias Seid, Fredrik Blix
Department of Computer and Systems Sciences
Stockholm University, Sweden
E-mail: (Ali, Naol, elias.seid, Fredrik) @dsv.su.se

***Abstract*—The increasing reliance of financial institutions on cloud infrastructures has amplified concerns surrounding regulatory compliance and cybersecurity, particularly in light of the EU's Digital Operational Resilience Act (DORA). This paper presents an experimental, empirical model designed to assess security misconfigurations in Amazon Web Services (AWS) and evaluate their alignment with DORA compliance requirements. Leveraging a Python-based scanning script built with the AWS Boto3 Software Development Kit (SDK), the study programmatically inspects critical AWS services—S3, Elastic Compute Cloud (EC2), Identity and Access Management (IAM), and Virtual Private Cloud (VPC)—within a controlled environment configured with known vulnerabilities. Each misconfiguration is automatically mapped to relevant DORA articles (Articles 5, 9, and 10) and accompanied by actionable remediation strategies. The results, visualised through a Streamlit dashboard and exportable PDF reports, demonstrate the tool's ability to detect compliance gaps in real time. Unlike previous work based on theoretical models or manual audits, this research offers a replicable, data-driven approach that bridges the gap between technical vulnerabilities and regulatory mandates. By doing so, it empowers financial institutions to strengthen their operational resilience and proactively align with emerging regulatory standards in dynamic cloud ecosystems.**

Keywords-Cloud Security; DORA Compliance; Financial Institutions; AWS Misconfigurations; Operational Resilience; Regulatory Technology (RegTech); Cybersecurity Governance Identity and Access Management (IAM)

I. Introduction

In the rapidly evolving landscape of financial services, cloud computing has become a fundamental component in modernising how institutions manage operations and deliver services to customers. Financial institutions worldwide are increasingly leveraging Cloud Service Providers (CSPs) for critical business functions such as data storage, payment processing, advanced analytics, and customer relationship management [24][38][40].

This transition to cloud-based solutions offers significant benefits, including scalability, cost efficiency, and enhanced service delivery. However, it also introduces new and complex security challenges that require continuous monitoring, risk assessment, and mitigation strategies [32]. DORA specifically mandates financial institutions to address these challenges by implementing comprehensive risk management frameworks for third-party cloud service providers and ensuring continuous cybersecurity threat monitoring [40].

Among these challenges, cloud misconfigurations have emerged as a leading cause of security breaches in financial institutions. Improperly configured cloud environments can expose sensitive data, create compliance gaps, and increase the risk of cyberattacks [48]. As organisations shift their infrastructure to the cloud, these misconfigurations—ranging from publicly accessible storage buckets and overly permissive IAM roles to mismanaged network security groups—have become a major security concern. Financial institutions, due to their reliance on cloud service providers, must proactively identify, assess, and remediate these security flaws to meet regulatory requirements and maintain operational resilience [6][16].

Recognising these risks, the European Union's Digital Operational Resilience Act (DORA) was introduced to strengthen the financial sector's resilience against Information and Communication Technology (ICT) risks. DORA, implemented in January 2023 and set to take full effect by January 2025, mandates financial institutions to establish comprehensive risk management frameworks for third-party cloud service providers, cybersecurity threat monitoring, and operational resilience. Ensuring compliance with DORA requires financial institutions to implement robust security controls, perform continuous monitoring, and mitigate cloud security risks to protect against operational disruptions and cyber threats [1][40].

While prior studies have explored general cloud security frameworks and compliance models (e.g., ISO/IEC 27001, National Institute of Standards and Technology (NIST)), there remains a lack of empirical, data-driven research that examines how cloud misconfigurations in AWS directly affect regulatory compliance under the recently enacted Digital Operational Resilience Act (DORA). Existing work tends to focus on theoretical models or survey-based risk assessments [27][37], offering limited insight into direct DORA compliance mapping.

This presents a critical research problem: financial institutions currently lack validated experimental models that systematically assess AWS misconfigurations and evaluate their implications for DORA compliance [27][36]. Traditional security assessments often rely on theoretical security models, self-reported case studies, or compliance-driven audits that do not capture real-time misconfiguration risks in AWS environments [27]. There is a lack of experimental research that empirically assesses cloud security vulnerabilities, particularly in financial institutions subject to regulatory compliance under DORA [40][44]. Additionally, many cybersecurity frameworks are designed for on-premise infrastructures and struggle to account for the dynamic, elastic, and multi-tenant nature of cloud computing [6].

Objective of this paper: The existing research on cloud security and financial regulations lacks empirical studies that specifically assess real-world AWS misconfigurations and their impact on DORA compliance, leaving financial institutions without actionable guidance [5][40][46]. Most literature remains theoretical or relies on manual audits, which do not account for the cloud's dynamic environment or enable continuous validation [27][51]. With the growing use of multi-cloud and hybrid-cloud architectures, new misconfiguration risks and third-party dependencies have emerged, yet these complexities remain underexplored, especially concerning DORA's third-party risk mandates [14][21][32][47]. Furthermore, the integration of automated security testing in financial cloud systems is limited, and there is a scarcity of research on programmatic detection and vulnerability mapping to regulatory frameworks, such as DORA [27][37]. Addressing this gap, the present study introduces a novel experimental model that identifies AWS misconfigurations and aligns them with DORA requirements using security scanning and compliance validation tools, offering empirical, data-driven insights to improve security posture and regulatory alignment.

This research contributes to both academic understanding and practical implementation by providing financial institutions with an automated, resilient approach to detect and remediate risks in a continuously evolving cloud landscape. This study aims to empirically assess cloud security misconfigurations in Amazon Web Services (AWS) within financial institutions and evaluate their alignment with the Digital Operational Resilience Act (DORA). By implementing a security scanning tool, the research seeks to identify key vulnerabilities, provide actionable insights for regulatory compliance, and strengthen operational resilience in dynamic cloud environments [16][21][38][40]. By answering the following research question: **How can an experimental security scanning model be utilised to identify common AWS misconfigurations and report their alignment with DORA compliance requirements?**

- Review existing literature to identify common AWS cloud security misconfigurations in financial institutions, focusing on S3, EC2, VPC, and IAM vulnerabilities.
- Develop a Python-based scanning tool using Boto3 to empirically assess real-world AWS misconfigurations and evaluate their impact in the context of DORA requirements.
- Map identified misconfigurations to DORA compliance gaps and proposed remediation strategies to enhance regulatory adherence and cloud security.

The remainder of this paper is structured as follows. Section 2 outlines the research baseline and related literature. Section 3 describes the methodology. Section 4 presents the results and key themes. Section 5 discusses the findings, and Section 6 concludes with implications and future research directions.

II. Research Baseline

The growing adoption of cloud computing has transformed how financial institutions manage infrastructure and deliver services, offering benefits such as scalability and efficiency [32]. However, this shift introduces complex cybersecurity risks—especially cloud misconfigurations such as exposed storage, permissive access controls, and insecure APIs—which can result in data breaches and non-compliance [16]. The EU's Digital Operational Resilience Act (DORA) mandates robust ICT risk management, continuous monitoring, and oversight of third-party providers to enhance operational resilience [21][40]. Yet, financial institutions struggle to meet these standards due to limited empirical research on real-world AWS misconfigurations and reliance on outdated manual assessments [37] [51]. To bridge this gap, the study introduces an experimental model that programmatically detects vulnerabilities in AWS components, such as S3, EC2, VPCs, and IAM policies, evaluating their alignment with DORA requirements. By leveraging automated security testing, it offers practical insights for enhancing compliance and resilience. The chapter also reviews existing literature on cloud security, regulatory demands, and assessment tools, highlighting the necessity of empirical approaches in today's evolving financial cloud landscape.

A. Cloud Security Risks in Financial Institutions

The adoption of cloud computing in financial services has enabled institutions to leverage technologies such as AI, ML, and big data analytics, driving innovation and operational efficiency [4][18]. However, this shift introduces complex security challenges, particularly as institutions integrate multiple cloud service providers (CSPs) and hybrid infrastructures [14][16][32]. Compliance with regulations such as the Digital Operational Resilience Act (DORA) has become essential, requiring continuous monitoring and robust security controls [16][21]. Misconfigurations in cloud environments—such as exposed S3 buckets, overly permissive EC2 security groups, flawed VPC configurations, and weak IAM policies—pose significant risks, often stemming from human error and lack of automation [8][37]. Financial institutions must move toward automated, proactive security assessment methods to reduce vulnerabilities and ensure DORA compliance. Studies highlight that cloud misconfigurations remain one of the most critical cybersecurity threats, often resulting in data breaches, regulatory violations, and reputational damage [16][29]. Common misconfigurations include public S3 access, lack of encryption, misconfigured security groups exposing open ports, and permissive IAM roles lacking MFA [43][52]. High-profile breaches—such as those affecting Capital One and Twilio—illustrate the real-world impact of these flaws [16]. VPC misconfigurations, such as permissive ACLs and disabled flow logs, further expose financial systems to threats and DORA non-compliance [21][34]. DORA mandates secure configurations, real-time monitoring, and effective incident response, and non-compliance can result in penalties and regulatory scrutiny [33][40]. As attackers increasingly exploit cloud weaknesses, systematic security validation and automated compliance tools are essential to safeguard financial data and maintain resilience in dynamic cloud ecosystems [27][37].

B. Cloud Security Compliance and Regulatory Challenges

Cloud security compliance presents a critical challenge for financial institutions, particularly under the EU's Digital Operational Resilience Act (DORA), which mandates continuous security monitoring, incident reporting, and risk mitigation for cloud-based infrastructures [21][33][40]. Articles 5, 9, and 10 of DORA require institutions to manage ICT risks, ensure secure configurations, and promptly report security incidents. However, traditional manual audits are periodic, reactive, and largely ineffective in detecting ephemeral or dynamic misconfigurations common in cloud environments [14][35][37]. Studies highlight the urgency for automated tools that enable real-time detection, secure configuration enforcement, and regulatory alignment, particularly as threats related to misconfigured APIs, access control, and third-party providers persist [16][40][48].

Emerging research supports the use of AI-driven security analytics and automated compliance tools such as AWS Config and Azure Policy to conduct continuous auditing and misconfiguration detection [3][27]. These tools leverage dynamic security enforcement, anomaly detection, and real-time risk scoring to proactively address vulnerabilities [10][41]. Despite the potential, integration across multi-cloud platforms remains difficult due to technical complexity, limited expertise, and high costs [12]. This study contributes to the field by developing a Python-based AWS scanning script that detects misconfigurations in S3, EC2, IAM, and VPC settings, then maps findings to DORA's regulatory framework. The results provide empirical support for transitioning from static, manual audits to automated compliance mechanisms, enabling financial institutions to better manage risks and meet evolving regulatory demands.

C. Security Assessments in Cloud Environments

As cloud infrastructures grow in complexity, financial institutions face increasing challenges in ensuring compliance and detecting security misconfigurations, prompting a shift from manual to automated cloud security testing [23]. Automated tools leverage programmatic data collection, API-driven analysis, and AI-enhanced threat detection to identify misconfigurations in real time, outperforming manual methods in speed and accuracy [9]. Native tools such as AWS Security Hub, GuardDuty, Config, and IAM Access Analyser support continuous compliance validation, while third-party solutions such as Prisma Cloud and CloudGuard enhance threat detection across multi-cloud environments [20][49]. Despite these tools' capabilities, challenges remain in interpreting automated findings within regulatory contexts such as DORA, which demands structured incident reporting, secure configurations, and continuous monitoring [21] [40]. Studies stress the need for hybrid models combining automation with expert validation to ensure accurate risk assessments [25][53]. Empirical research is increasingly recognised as essential in cloud security, moving beyond theoretical models and survey-based studies to produce data-driven insights into real-world misconfigurations [39]. Experimental methods deploy cloud environments to simulate and observe security flaws, using tools such as the AWS Boto3 SDK for automated scans and compliance mapping [30]. While traditional research often neglects regulatory alignment, empirical approaches directly link misconfigurations to mandates such as DORA, offering measurable compliance validation and reproducible security testing [9][27]. Despite progress, gaps remain in systematically quantifying the risk severity of misconfigurations and incorporating automated assessments into compliance workflows. This study addresses these gaps by developing and testing a Python-based AWS scanning model, aiming to enhance operational resilience and regulatory adherence through experimental, programmatic cloud security evaluation.

D. Empirical Cloud Security Assessment Model

While existing research has advanced understanding of cloud security and compliance in financial institutions, a critical gap remains in empirically validating how real-world AWS misconfigurations impact regulatory requirements—particularly under the EU's Digital Operational Resilience Act (DORA) [17][27]. DORA mandates continuous risk monitoring, third-party oversight, and operational resilience, recognising cloud service providers as key vulnerabilities in modern finance [26]. However, most prior studies focus on high-level governance, theoretical models, or qualitative assessments without conducting experimental evaluations of AWS-specific security flaws [7][22]. As financial institutions continue to rely on periodic manual audits, they fail to meet DORA's need for continuous, automated security validation [9][28]. This study addresses those limitations by developing an experimental, Python-based security scanning model using the AWS Boto3 SDK to detect real-world misconfigurations and map them directly to DORA compliance mandates. Unlike previous works that discuss threat frameworks such as MITRE ATT&CK or general CTI practices [11][50], this research offers actionable, data-driven insights through structured testing in live AWS environments. It also considers risks introduced by multi-cloud and hybrid-cloud infrastructures—an area underexplored in the context of DORA's third-party ICT risk requirements [13]. By integrating compliance validation with technical scanning, the model enables financial institutions to proactively identify, quantify, and remediate misconfigurations, contributing both to regulatory adherence and enhanced cloud security governance.

Given the lack of empirical research on how AWS misconfigurations impact compliance with the Digital Operational Resilience Act (DORA), this study justifies a controlled experiment in a real AWS environment to systematically detect, analyse, and classify security vulnerabilities. Using a custom Python-based scanning tool developed with the Boto3 SDK, the research provides real-time, proactive security validation that surpasses traditional manual audits. The experiment directly maps misconfigurations to DORA's operational resilience requirements, offering data-driven recommendations for remediation and regulatory alignment. It incorporates reproducible testing, a Streamlit-based visualisation dashboard, and automated PDF reporting to translate complex findings into actionable insights. This approach bridges the gap between

technical vulnerabilities and regulatory mandates, making it one of the first empirical studies to validate AWS security risks against DORA, ultimately enhancing compliance and operational resilience, and reducing financial institutions' exposure to cyber threats and penalties.

III. Method Application

This study adopts an experimental, empirical approach to evaluate cloud security misconfigurations and their implications for compliance with the Digital Operational Resilience Act (DORA) in financial institutions. Conducted within a controlled AWS environment, the research uses a custom Python-based scanning script built with the Boto3 SDK [30] to programmatically collect and assess real-time configuration data from key services such as Amazon S3, EC2, IAM, and VPC. By intentionally introducing known misconfigurations—such as publicly accessible S3 buckets, overly permissive EC2 rules, excessive IAM privileges, and exposed VPC routes—the script detects vulnerabilities and maps each finding to specific DORA compliance clauses. Unlike theoretical or survey-based studies [28], this method produces primary data and delivers actionable, data-driven insights that support regulatory alignment, continuous monitoring, and operational resilience [21][40]. Though direct institutional collaboration was beyond scope, the modular and replicable methodology offers a foundation for future industry use and potential integration into automated compliance pipelines.

Data Analysis Method: This study utilises a rule-based analysis approach to identify cloud security misconfigurations in a live AWS environment and assess their alignment with the Digital Operational Resilience Act (DORA). A custom Python script, built with the AWS Boto3 SDK [30], collects real-time configuration data and evaluates it against a predefined set of rules based on AWS security best practices and DORA requirements [33][40]. Misconfigurations—such as publicly accessible S3 buckets or unencrypted storage—are flagged and automatically mapped to relevant DORA articles (e.g., Article 5 on ICT risk management, Article 9 on secure configurations) using a built-in lookup table. For each violation, the script also generates remediation recommendations aligned with both AWS and DORA standards. To validate the methodology, the script was tested in a controlled AWS environment pre-loaded with known misconfigurations. Outputs, including detected issues, mapped DORA clauses, and corrective actions, were reviewed and cross-checked against AWS Config reports to ensure accuracy. This rule-based method was chosen over statistical or qualitative techniques due to its direct alignment with the study's goal of evaluating compliance and generating actionable insights [27][37]. Its structured, automated logic makes it scalable, reproducible, and well-suited for regulatory security assessments in cloud environments [9][53].

Controlled Experiment Set-Up: This study conducts a controlled experiment in an AWS environment to empirically assess cloud security misconfigurations and their compliance—as shown in Figure 1—with the Digital Operational Resilience Act (DORA). A dedicated test environment was set up with intentionally introduced vulnerabilities—such as public S3 buckets without encryption, overly permissive EC2 security groups, IAM roles with wildcard permissions, and misconfigured VPCs with disabled flow logs and unrestricted traffic [16][29]. A custom Python script using the Boto3 SDK [30] scans these configurations against security best practices and DORA requirements [33][40], flagging violations and mapping them to specific DORA articles. The experiment leverages services such as EC2, S3, IAM, and VPC, with data processed using Pandas and formatted in JSON. The setup, built in VS Code with AWS CLI and Cloud Terminal, creates a reproducible and realistic environment for testing regulatory cloud security compliance. Moreover, a Python-based security scanning script using the AWS Boto3 SDK [30] evaluates key AWS services for misconfigurations and assesses their compliance with DORA Articles 5, 9, and 10 [21][33]. The script conducts API-driven checks on S3 buckets (public access, encryption, logging); EC2 security groups (open ports); IAM policies (excessive permissions, lack of Multi-Factor Authentication (MFA)); and VPC settings (routing tables, ACLs) to detect vulnerabilities. Each misconfiguration is automatically mapped to relevant DORA clauses, ensuring regulatory clarity and actionable compliance alignment [27][37].

To enhance usability, the results are visualised through a Streamlit dashboard that presents service-specific findings, associated DORA violations, and recommended remediation steps [9]. The dashboard also generates comprehensive PDF reports summarising vulnerabilities and compliance gaps, enabling real-time monitoring and audit support. The experiment is designed for easy replication across AWS environments, providing a standardised, empirically validated model for improving cloud security governance and regulatory adherence in financial institutions [27][40]. The complete technical implementation details, source code, and stepby- step instructions for replicating this experimental setup are available in the project's public GitHub repository [2].

IV. Experimental Result

The scanner was deployed in a controlled AWS environment pre-configured with common misconfigurations to evaluate its effectiveness in identifying security weaknesses across S3, EC2, IAM, and VPC services and mapping them to relevant DORA articles. The automated scan produced categorised findings—S3, EC2 Security Group, IAM, and VPC issues—each linked to DORA Articles 5, 9, or 10, highlighting their regulatory relevance. The results, visualised through a Streamlit dashboard and compiled into a PDF report, include remediation recommendations and serve as the study's core empirical evidence, demonstrating the tool's capability to enhance cloud security and support compliance in financial institutions.

S3 Compliance Issues The scan targeted an S3 bucket named "bucket-misconfigured", created specifically for this experiment with known vulnerabilities. Two significant misconfigurations were identified: **Public Access Enabled:** The scanner found misconfigured public access block settings on the S3 bucket,

risking unauthorised data exposure. This was mapped to DORA Article 9, which mandates secure cloud configurations. The tool recommended enabling all four Public Access Block settings to align with AWS best practices and enhance operational resilience. **Bucket Logging Disabled:** The absence of server access logging was flagged, violating DORA Article 10's requirements for continuous monitoring and audit trails. The tool advised enabling logging to support access traceability, security governance, and incident response. These S3 findings, detected within the controlled environment, demonstrate the scanner's ability to identify fundamental configuration errors that violate core DORA principles related to secure configurations and governance.

EC2 Security Group Issues: Within the EC2 Security Group configurations (Figures 2, 3, and 4 illustrate typical EC2 security group issues), the scanner identified three critical issues, all associated with DORA Article 9 due to their impact on secure cloud setups: **Unrestricted SSH Access:** SSH (port 22) was open to all IPs (0.0.0.0/0), posing a major risk of unauthorised remote access. **Unrestricted ICMP Access:** ICMP traffic was allowed from any IP, increasing vulnerability to network reconnaissance. **Unrestricted RDP Access:** RDP (port 3389) was open to the internet, exposing systems to potential remote exploitation. The scanner flagged overly permissive EC2 security group rules but did not provide detailed remediation steps, highlighting a limitation in its firewall logic. Still, the detection aligns with DORA's requirements for strict access controls and secure network configurations. In the IAM category, multiple misconfigurations were identified and mapped to DORA Article 5, including wildcard permissions in AWS-managed roles and the absence of Multi-Factor Authentication (MFA) for several user accounts. While the tool consistently recommended enabling MFA, it lacked specific guidance for reviewing default service-linked roles. Additionally, inactive accounts were flagged for review to reduce the attack surface. These findings reveal critical identity and access management gaps that pose compliance risks under DORA. **VPC Issues:** The scan of VPC configurations revealed network-level misconfigurations, mapped to either DORA Article 9 (Secure Configurations) or Article 10 (Governance and Monitoring): **Default Route to Internet Gateway:** A route table pointed all traffic (0.0.0.0/0) to an Internet Gateway, which is acceptable for public subnets but risks exposing private ones—violating DORA Article 9 on secure network segmentation. The tool recommended validating intent and using a NAT Gateway if needed. **Overly Permissive Network ACL:** A subnet's ACL allowed all inbound/outbound traffic (0.0.0.0/0), weakening segmentation controls under Article 9. Restricting traffic to required protocols was advised. **VPC Flow Logs Disabled:** Flow logs were not enabled, breaching DORA Article 10 on monitoring and incident response. The scanner recommended enabling them for better visibility and governance.

The AWS Security Scanner's findings in the controlled experiment reveal a high prevalence of critical misconfigurations across S3, EC2, IAM, and VPC services, confirming the complexity and risk of securing cloud environments. These misconfigurations—such as public S3 buckets, open EC2 ports, overly permissive IAM roles, and disabled logging—were systematically mapped to DORA Articles 5, 9, and 10, highlighting direct regulatory non-compliance [33][40]. The issues reflect systemic weaknesses such as poor access control, insufficient monitoring, and lax network security, all of which undermine operational resilience. These are not isolated flaws but are indicative of broader security governance gaps driven by default settings, limited oversight, and human error, aligning with prior research [42]. Collectively, the vulnerabilities pose significant risks—ranging from data breaches to operational disruption—and demonstrate the scanner's effectiveness in linking technical security gaps to regulatory obligations under DORA [21][27].

V. CONCLUSION AND FUTURE WORK

Unique contributions and addressing research gaps This study makes key contributions by addressing research gaps identified in Section 1.3, particularly the lack of practical, DORA-specific tools for assessing cloud security risks in financial institutions. It introduces a novel, open-source AWS Security Scanner that integrates DORA compliance mapping for key services, bridging the gap between technical misconfigurations and regulatory mandates. Unlike prior work focused on general cloud security or high-level DORA governance [33][40], this tool includes an interactive dashboard and PDF reporting to provide actionable insights directly linked to compliance needs. Moreover, the research delivers empirical validation within a controlled AWS environment, moving beyond theoretical or survey-based studies [16][19] to demonstrate how specific misconfigurations directly violate DORA Articles 5, 9, and 10 [21][27]. By systematically connecting technical issues to regulatory clauses, the study helps bridge the technical–regulatory divide and supports continuous compliance monitoring. It equips financial institutions with a replicable methodology and real-world remediation guidance, offering both a valuable tool and fresh empirical evidence to enhance operational resilience under DORA.

This paper developed and validated the AWS Security Scanner—an experimental, open-source tool designed to detect common cloud misconfigurations in AWS and map them to specific DORA compliance requirements [27][30]. Through controlled testing, the scanner effectively identified vulnerabilities in S3, EC2, IAM, and VPC services, demonstrating its ability to highlight direct regulatory implications [21][33]. The study contributes a novel compliance-aware tool, offers empirical validation, bridges technical and regulatory gaps, and provides actionable insights for financial institutions. It addresses critical research gaps and reinforces the need for automated security solutions that enhance operational resilience and regulatory adherence in the cloud-driven financial sector [9][37].

Future research could enhance the tool's utility by expanding support to other cloud platforms, such as Azure and Google Cloud, enabling broader misconfiguration detection across

VPC Issues

Resource	Issue	DORA Mapping	Recommendation
rtb-0107bdba3e54090b2	Default route to an Internet Gateway detected; verify if intended for public subnets.	Article 9 (Secure Cloud Configurations)	Ensure that default routes to an Internet Gateway are only associated with public subnets. For private subnets requiring outbound internet access, use a NAT Gateway or NAT Instance.
acl-0fec7c2a77c5aca55	Overly permissive rule allowing all traffic from 0.0.0.0/0 detected.	Article 9 (Secure Cloud Configurations)	Tighten Network ACL rules to restrict inbound and outbound traffic to only necessary protocols, ports, and specific source/destination IP ranges, following the principle of least privilege.
acl-0fec7c2a77c5aca55	Overly permissive rule allowing all traffic from 0.0.0.0/0 detected.	Article 9 (Secure Cloud Configurations)	Tighten Network ACL rules to restrict inbound and outbound traffic to only necessary protocols, ports, and specific source/destination IP ranges, following the principle of least privilege.
vpc-035e9a523f34825b4	VPC Flow Logs are not enabled, which may hinder network traffic monitoring.	Article 10 (Incident Reporting & Security Governance)	Enable VPC Flow Logs for the VPC to capture IP traffic information. This is crucial for network monitoring, security analysis, and troubleshooting.

Figure 1. S3 Compliance Issues

VPC Issues

Resource	Issue	DORA Mapping	Recommendation
rtb-0107bdba3e54090b2	Default route to an Internet Gateway detected; verify if intended for public subnets.	Article 9 (Secure Cloud Configurations)	Ensure that default routes to an Internet Gateway are only associated with public subnets. For private subnets requiring outbound internet access, use a NAT Gateway or NAT Instance.
acl-0fec7c2a77c5aca55	Overly permissive rule allowing all traffic from 0.0.0.0/0 detected.	Article 9 (Secure Cloud Configurations)	Tighten Network ACL rules to restrict inbound and outbound traffic to only necessary protocols, ports, and specific source/destination IP ranges, following the principle of least privilege.
acl-0fec7c2a77c5aca55	Overly permissive rule allowing all traffic from 0.0.0.0/0 detected.	Article 9 (Secure Cloud Configurations)	Tighten Network ACL rules to restrict inbound and outbound traffic to only necessary protocols, ports, and specific source/destination IP ranges, following the principle of least privilege.
vpc-035e9a523f34825b4	VPC Flow Logs are not enabled, which may hinder network traffic monitoring.	Article 10 (Incident Reporting & Security Governance)	Enable VPC Flow Logs for the VPC to capture IP traffic information. This is crucial for network monitoring, security analysis, and troubleshooting.

Figure 2. EC2 Security Group Issues

VPC Issues

Resource	Issue	DORA Mapping	Recommendation
rtb-0107bdba3e54090b2	Default route to an Internet Gateway detected; verify if intended for public subnets.	Article 9 (Secure Cloud Configurations)	Ensure that default routes to an Internet Gateway are only associated with public subnets. For private subnets requiring outbound internet access, use a NAT Gateway or NAT Instance.
acl-0fec7c2a77c5aca55	Overly permissive rule allowing all traffic from 0.0.0.0/0 detected.	Article 9 (Secure Cloud Configurations)	Tighten Network ACL rules to restrict inbound and outbound traffic to only necessary protocols, ports, and specific source/destination IP ranges, following the principle of least privilege.
acl-0fec7c2a77c5aca55	Overly permissive rule allowing all traffic from 0.0.0.0/0 detected.	Article 9 (Secure Cloud Configurations)	Tighten Network ACL rules to restrict inbound and outbound traffic to only necessary protocols, ports, and specific source/destination IP ranges, following the principle of least privilege.
vpc-035e9a523f34825b4	VPC Flow Logs are not enabled, which may hinder network traffic monitoring.	Article 10 (Incident Reporting & Security Governance)	Enable VPC Flow Logs for the VPC to capture IP traffic information. This is crucial for network monitoring, security analysis, and troubleshooting.

Figure 3. IAM Issues

VPC Issues

Resource	Issue	DORA Mapping	Recommendation
rtb-0107bdba3e54090b2	Default route to an Internet Gateway detected; verify if intended for public subnets.	Article 9 (Secure Cloud Configurations)	Ensure that default routes to an Internet Gateway are only associated with public subnets. For private subnets requiring outbound internet access, use a NAT Gateway or NAT Instance.
acl-0fec7c2a77c5aca55	Overly permissive rule allowing all traffic from 0.0.0.0/0 detected.	Article 9 (Secure Cloud Configurations)	Tighten Network ACL rules to restrict inbound and outbound traffic to only necessary protocols, ports, and specific source/destination IP ranges, following the principle of least privilege.
acl-0fec7c2a77c5aca55	Overly permissive rule allowing all traffic from 0.0.0.0/0 detected.	Article 9 (Secure Cloud Configurations)	Tighten Network ACL rules to restrict inbound and outbound traffic to only necessary protocols, ports, and specific source/destination IP ranges, following the principle of least privilege.
vpc-035e9a523f34825b4	VPC Flow Logs are not enabled, which may hinder network traffic monitoring.	Article 10 (Incident Reporting & Security Governance)	Enable VPC Flow Logs for the VPC to capture IP traffic information. This is crucial for network monitoring, security analysis, and troubleshooting.

Figure 4. PC Issues

hybrid and multi-cloud setups [14][32]. Enhancing DORA coverage and integrating other regulatory frameworks such as GDPR or PCI-DSS would provide financial institutions with more comprehensive compliance insights [21][33]. Incorporating AI-driven remediation could offer context-aware, prioritised recommendations [41], while automating the tool for continuous monitoring and real-time fixes would improve efficiency [9][53]. Finally, deploying the scanner in live financial environments would validate its real-world effectiveness and guide further optimisation [27].

REFERENCES

[1] A. Abu, T. Smith, and T. Carlsen, "Cloud risk management in financial institutions: A compliance-focused approach," Journal of Financial Compliance , vol. 12, no. 3, pp. 34–42, 2018.

[2] N. Mengistu, "AWS Security Scanner," GitHub Repository , 2025. [Online]. Available: https://github.com/NaolMengistu/AWS-security-scanner?tab=readme-ovfile. [Accessed: 24-Oct-2025].

[3] M. M. Alani, "Guide to cloud computing principles and practice," Springer , 2016.

[4] H. Alavizadeh et al., "Security compliance automation in cloud environments using anomaly detection," Computers & Security, vol. 94, pp. 101814, 2020.

[5] A. Alhchaimi, "Leveraging cloud technologies for AI-driven finance: Risks and opportunities," Financial Technology Review, vol. 22, no. 1, pp. 45–58, 2024.

[6] D. Anson, "Cloud security automation and regulatory readiness," International Journal of Information Security, vol. 18, no. 2, pp. 123–136, 2024.

[7] S. Arowolo et al., "Security challenges in multi-tenant cloud environments," Cloud Security Review, vol. 10, no. 2, pp. 87–99, 2017.

[8] M. Backes et al., "Automated detection of cloud misconfigurations using compliance policies," Proc. ACM Cloud Security Workshop , pp. 88–95, 2019.

[9] S. Bleikertz, C. Vogel, and T. Gross, "Cloud configuration vulnerabilities," IEEE Transactions on Dependable and Secure Computing , vol. 11, no. 3, pp. 212–225, 2014.

[10] M. Campbell et al., "Real-time compliance validation in cloud-native security," Journal of Cybersecurity Automation, vol. 19, no. 1, pp. 77–92, 2024.

[11] P. Chethan, et al., "Machine learning for misconfiguration detection in cloud environments," Journal of Cloud Computing , vol. 11, no. 1, pp. 33–47, 2023.

[12] A. Coppola et al., "Cyber threat intelligence frameworks and regulatory compliance," Cyber Risk Studies, vol. 29, no. 2, pp. 59–72, 2023.

[13] R. Devan et al., "Challenges in multi-cloud compliance monitoring," Information Systems and Compliance Journal, vol. 17, no. 4, pp. 205–218, 2024.

[14] C. Dietrich et al., "Multi-cloud infrastructure and third-party risks in finance," European Journal of Financial Regulation, vol. 8, no. 3, pp. 188–199, 2018.

[15] R. Gade, "Multi-cloud architecture and compliance challenges," Journal of Cloud Infrastructure , vol. 5, no. 2, pp. 121–134, 2022.

[16] S. Geiger et al., "Third-party dependencies in cloud environments," Risk and Resilience Journal, vol. 14, no. 2, pp. 103–119, 2016.

[17] D. Guffey and Y. Li, "Cloud misconfigurations in financial services: A threat landscape review," Journal of Information Security , vol. 14, no. 1, pp. 1–19, 2023.

[18] R. Gudimetla et al., "Empirical security assessments in cloud environments," Cloud Security Analytics, vol. 9, no. 3, pp. 142–155, 2022.

[19] Z. Han et al., "Big data analytics in cloud-enabled financial systems," Journal of Applied Finance and Analytics, vol. 16, no. 2, pp. 44–57, 2023.

[20] M. Jansson, "Periodic audits vs. continuous monitoring in cloud compliance," Journal of Cybersecurity Practice, vol. 7, no. 3, pp. 55–64, 2021.

[21] D. Kanikathottu, "AWS-native tools for cloud compliance monitoring," Amazon Web Services Technical Reports, 2020.

[22] A. Karakasilioti et al., "DORA compliance in dynamic cloud infrastructures," Financial Cybersecurity Review, vol. 11, no. 1, pp. 28–46, 2024.

[23] R. Khanal and B. Maharjan, "DORA and the future of cloud regulation," Journal of Regulatory Technology, vol. 20, no. 1, pp. 99–112, 2024.

[24] M. Kunz et al., "Automating cloud risk assessments," Cybersecurity Automation Journal, vol. 15, no. 4, pp. 211–226, 2022.

[25] C. Lampe et al., "The evolution of cloud computing in finance," Journal of Banking Technology, vol. 4, no. 1, pp. 33–47, 2012.

[26] V. Mahida, "Challenges in interpreting automated security findings for compliance," Information Security Journal , vol. 12, no. 2, pp. 65–77, 2024.

[27] M. Maryska, P. Doucek, and L. Nedomová, "DORA and its impact on EU financial institutions,"European Cybersecurity Law Review , vol. 5, no. 1, pp. 22–38, 2024.

[28] I. Martseniuk et al., "Empirical evaluation of AWS misconfigurations under DORA," Journal of Financial Information Systems , vol. 10, no. 1, pp. 1–15, 2024.

[29] A. Mishra et al., "Manual vs. automated compliance auditing in finance," Compliance Technology Review, vol. 13, no. 2, pp. 72–86, 2022.

[30] R. Mohammed and R. Khare, "Misconfigured networks in regulated cloud environments," Journal of Network Security , vol. 19, no. 3, pp. 143–155, 2024.

[31] T. Mukherjee et al., "Using Boto3 for automated cloud security validation," Proc. CloudSec Conference, pp. 134–141, 2022.

[32] K. Namuduri, "Risk assessment approaches in financial cybersecurity," Journal of Information Assurance, vol. 6, no. 1, pp. 11–25, 2013.

[33] H. Nutalapati, "Cloud transformation in financial services," *International Journal of FinTech Innovation, vol. 9, no. 1, pp. 37–49, 2024.

[34] K. Parchimowicz, "Regulatory impact of DORA on the financial sector," European Journal of Financial Regulation, vol. 12, no. 1, pp. 50–66, 2024.

[35] M. Patibandla, "Network exposure risks in financial clouds," Journal of Secure Computing, vol. 10, no. 4, pp. 188–201, 2024.

[36] V. Patil et al., "Cloud misconfigurations and reactive auditing," Cyber Risk and Compliance Quarterly, vol. 6, no. 2, pp. 90–102, 2019.

[37] D. Ponnusamy, "Validating AWS misconfigurations through simulation," Information Assurance Bulletin, vol. 21, no. 2, pp. 101–114, 2023.

[38] M. Rahman et al., "Cloud security automation and DORA," Journal of Regulatory Compliance , vol. 17, no. 1, pp. 48–60, 2024.

[39] S. Rana et al., "Cloud compliance in EU financial institutions," Journal of Finance and Cloud Security , vol. 15, no. 2, pp. 27–41, 2023.

[40] H. Rathore, "Experimental approaches in cloud security research," Cloud Research Bulletin, vol. 18, no. 1, pp. 65–77, 2024.

[41] L. Scott, "Cloud regulation under DORA: A technical overview," European Cybersecurity Studies, vol. 9, no. 4, pp. 22–35, 2021.

[42] A. Sodiya et al., "AI-enhanced IAM policy enforcement in cloud," Journal of Information Policy and Automation, vol. 23, no. 3, pp. 112–124, 2024.

[43] G. Stergiopoulos, et al., "Human error and cloud security risks," Computers & Security vol. 77, pp. 45–60, 2018.

[44] S. Talluri, "IAM vulnerabilities in regulated cloud environments," Journal of Cloud Identity, vol. 14, no. 2, pp. 84–97, 2023.

[45] K. Torkura and C. Meinel, "Cloud computing compliance challenges in the EU," IT Governance Journal, vol. 6, no. 2, pp. 22–37, 2015.

[46] K. Torkura et al., "Dynamic validation in multitenant cloud environments," Cloud Computing Advances, vol. 8, no. 3, pp. 100–115, 2021.

[47] M. Uddin, M. Ali, and R. Hassan, "Cloud governance for financial institutions," Financial IT Journal, vol. 11, no. 2, pp. 66–80, 2020.

[48] J. Valbo, "DORA and cloud supply chain security," Journal of Finance & Infrastructure, vol. 9, no. 4, pp. 58–73, 2023.

[49] S. Van Ede et al., "Third-party risks in EU cloud regulation," Journal of Cyber Governance, vol. 13, no. 1, pp. 31–45, 2022.

[50] R. Venkat Soma, "Open-source scanning tools for multi-cloud," International Journal of Open Cybersecurity, vol. 5, no. 1, pp. 119–132, 2024.

[51] A. Verdet et al., "Threat intelligence models and compliance mapping," CTI and Governance Review, vol. 8, no. 1, pp. 93–107, 2023.

[52] F. Wenge et al., "Limitations of manual cloud security audits,"Journal of Information Risk, vol. 7, no. 3, pp. 44–59, 2014.

[53] Y. Wu and J. Feng, "Enforcing MFA in AWS cloud," Journal of Cyber Identity and Access, vol. 12, no. 3, pp. 78–89, 2021.

[54] R. Xiong and Y. Bu, "Hybrid security validation in cloud compliance," International Journal of Cloud Security, vol. 19, no. 1, pp. 23–38, 2024.