



University of Wales Trinity Saint David

MASTER'S PROJECT REPORT

A Theoretical Risk-Scoring Model for Cloud IAM Complexity

Shamsuddin Mahmud

Student ID: 2432880

MSc Cyber Security and Digital Forensics

Supervisor: Ramzi Djemai

September 2026

Declaration and Consent

I declare that this report, “**A Theoretical Risk-Scoring Model for Cloud IAM Complexity,**” is my own original work and has been completed in accordance with the academic and ethical requirements of the University of Wales Trinity Saint David.

All sources used in this report have been appropriately acknowledged and referenced. This research is based on published academic literature and does not involve human participants, personal data, confidential organisational information, or live testing on operational systems.

I confirm that the work submitted is accurate to the best of my knowledge and consent to its submission for final academic assessment.

Student Name: Shamsuddin Mahmud
Student Number: 2432880

Abstract

Cloud Identity and Access Management (IAM) environments are becoming increasingly complex due to growing numbers of identities, roles, permissions, policies, trust relationships, contextual conditions, and distributed resources. This complexity can make effective access difficult to understand and manage, increasing the likelihood that excessive permissions, policy weaknesses, governance failures, or privilege-escalation paths remain undetected.

This study develops a theoretical risk-scoring model for assessing security risk associated with cloud IAM complexity. A structured review of academic studies was used to identify and analyse relevant factors from cloud IAM, access-control models, IAM metrics, policy verification, privilege escalation, distributed authorization, context-aware access control, reachability analysis, and attack-graph research. The identified factors were consolidated into seven dimensions: Structural Complexity, Policy Quality and Maintainability Weakness, Permission Exposure, Privilege Propagation, Dynamic and Contextual Complexity, Governance Weakness, and Asset Criticality.

The proposed model separates IAM complexity from direct security exposure and treats complexity as a potential risk amplifier rather than a vulnerability. Normalized indicators are combined into complexity and exposure components, which are then used to produce an explainable overall risk score adjusted by asset criticality.

The study contributes a literature-grounded framework that integrates previously separate IAM complexity and security concepts into a single theoretical assessment model. As the model has not yet been empirically validated, its weights, thresholds, and risk classifications are considered provisional and require future testing using real or representative cloud IAM environments.

Table of Contents

Declaration and Consent	2
Abstract	3
Chapter 1 - Introduction	1
1.1 Aim	1
1.2 Objectives	1
1.3 Problem Statement.....	1
1.4 Significance of the Study	2
1.5 Expected Outcomes.....	2
1.6 Research Gap	2
1.7 Research Questions	3
1.8 Research Question Traceability Matrix.....	4
Chapter 2 - Literature Review	6
2.1 Foundations and Evolution of Access-Control Models.....	7
2.1.1 Role-Based Access Control	7
2.1.2 Attribute-Based Access Control.....	8
2.1.3 Hybrid and Policy-Based Access Control	9
2.2. IAM Requirements and Governance in Cloud Environments	9
2.2.1 Enterprise IAM Requirements	9
2.2.2 Identity Lifecycle Complexity	10
2.2.3 Access Reviews and Governance Burden	11
2.3. IAM Metrics, Policy Complexity, and Policy Quality	11
2.3.1 Authorization Accuracy	11
2.3.2 Policy Complexity	12
2.3.3 Redundancy	13
2.3.4 Understandability and Maintainability	13
2.3.5 Automation	14
2.4 IAM Misconfiguration, Excessive Privilege, and Privilege Escalation.....	14
2.4.1 Excessive Permission	14
2.4.2 Privilege Escalation	15
2.4.3 Limitations of Existing Detection Approaches.....	15
2.5 Formal Verification of IAM Policies	16

2.6 Graph-Based Modelling of IAM Complexity and Risk	17
2.6.1 Reachability Analysis	17
2.6.2 Network Vulnerability and Attack Graphs.....	18
2.6.3 Scalable Attack-Graph Generation.....	18
2.6.4 Graph Complexity as a Risk Indicator	18
2.7 Distributed, Fog, and Context-Aware Access-Control Complexity	19
2.7.1 Distributed Authorization	19
2.7.2 Fog Computing	20
2.7.3 Context-Aware Access Control	20
2.8 Synthesis of the Literature.....	21
2.8.1 Structural Complexity	21
2.8.2 Logical Complexity	21
2.8.3 Administrative Complexity.....	21
2.8.4 Dynamic Complexity	22
2.8.5 Exposure Complexity	22
2.8.6 Comparative Analysis of Reviewed Studies	22
Chapter 3 - Methodology.....	27
3.1 Research Design	27
3.2 Literature Review and Data Extraction.....	27
3.3 Identification of Model Dimensions.....	27
3.4 Model Development.....	28
3.5 Model Evaluation	28
3.6 Limitations and Validity.....	29
Chapter 4 - Proposed Cloud IAM Complexity Risk-Scoring Model.....	30
4.1 Model Overview	30
4.2 Final Risk Dimensions.....	30
4.3 Indicators and Metrics	31
4.3.1 Structural Complexity	31
4.3.2 Policy Quality and Maintainability Weakness.....	32
4.3.3 Permission Exposure	32
4.3.4 Privilege Propagation	32
4.3.5 Dynamic and Contextual Complexity.....	33

4.3.6 Governance Weakness	33
4.3.7 Asset Criticality	33
4.4 Metric Normalization	34
4.5 Dimension Scoring	35
4.6 Complexity and Exposure Components	36
4.7 Final Cloud IAM Complexity Risk Score	36
4.8 Risk Classification	37
4.9 Worked Hypothetical Example.....	37
4.10 Model Interpretation.....	38
4.11 Model Limitations and Validation Requirements	39
Chapter 5 - Discussion and Evaluation.....	40
5.1 Discussion of Findings	40
5.2 Evaluation of the Proposed Model	41
5.2.1 Literature Coverage.....	41
5.2.2 Logical Coherence	41
5.2.3 Traceability.....	42
5.2.4 Explainability.....	42
5.2.5 Measurability	42
5.2.6 Distinctiveness	42
5.2.7 Sensitivity	43
5.3 Answers to the Research Questions.....	43
5.4 Comparison with Existing Approaches.....	44
5.5 Limitations of the Study.....	45
5.6 Practical and Research Implications.....	45
Chapter 6 - Conclusion and Future Work.....	47
6.1 Conclusion	47
6.2 Achievement of Aim and Objectives	47
6.3 Research Contribution	48
6.4 Future Work.....	48
References.....	49

Chapter 1 - Introduction

1.1 Aim

The aim of this research is to develop a theoretical risk-scoring model for assessing security risks associated with Identity and Access Management (IAM) complexity in cloud environments. The proposed model will synthesize measurable IAM complexity and security factors identified in existing literature, including policy complexity, excessive permissions, privilege propagation, access-control relationships, governance weaknesses, and exposure to critical resources, to provide a structured and explainable basis for evaluating cloud IAM risk.

1.2 Objectives

To achieve the aim of developing a theoretical risk-scoring model for cloud IAM complexity, this study will pursue four consolidated objectives:

Review: To systematically review the selected literature on cloud IAM, access-control models, IAM metrics, policy quality, privilege escalation, distributed authorization, and graph-based security analysis in order to identify existing approaches and relevant complexity-related factors.

Analyse: To analyse and classify the factors that contribute to cloud IAM complexity and determine how these factors relate to security risk, including policy misconfiguration, excessive privilege, privilege propagation, governance weaknesses, contextual complexity, and exposure of critical resources.

Build: To develop an explainable theoretical risk-scoring model that organizes the identified IAM complexity and security indicators into measurable dimensions and provides a structured method for combining them into an overall cloud IAM complexity-risk assessment.

Evaluate: To evaluate the proposed theoretical model in terms of its literature coverage, conceptual coherence, traceability, explainability, assumptions, and limitations, while identifying the empirical validation required before the model could be applied operationally.

1.3 Problem Statement

Cloud IAM environments can become difficult to manage as the number of identities, roles, permissions, policies, resources, and trust relationships increases. This complexity can obscure excessive permissions, policy misconfigurations, ineffective access reviews, and privilege-escalation paths [3], [5]-[7].

Existing studies address IAM metrics, policy verification, privilege escalation, reachability, and attack graphs separately [3], [5]-[7], [12], [14]. However, the reviewed literature does not provide an integrated method for assessing how IAM complexity contributes to overall security risk.

This study therefore addresses the lack of an explainable theoretical model that combines IAM complexity, policy quality, permission exposure, privilege propagation, governance weakness, contextual complexity, and critical-resource exposure into a structured risk score.

1.4 Significance of the Study

This study contributes by bringing together concepts that are currently distributed across different areas of IAM research. It distinguishes **complexity from risk**, recognizing that a large IAM environment is not necessarily insecure, while a small configuration may still contain serious exposure.

The proposed model will combine relevant IAM metrics, policy-quality measures, privilege-escalation indicators, and graph-based exposure analysis into a single explainable framework. This may support more structured risk prioritization and provide a foundation for future empirical validation.

1.5 Expected Outcomes

The expected outcome is a **theoretical Cloud IAM Complexity Risk-Scoring Model** supported by the reviewed literature. The study is expected to:

1. Identify and classify the main dimensions of cloud IAM complexity.
2. Define measurable indicators for each dimension.
3. Develop a structured method for combining these indicators into an overall risk score.
4. Provide traceability between the overall score and its contributing factors.
5. Evaluate the model for conceptual coherence, coverage, and explainability.

1.6 Research Gap

Existing research provides substantial knowledge about individual aspects of IAM and access-control security, but there is a lack of an integrated approach for quantifying the security risk associated specifically with cloud IAM complexity.

Existing studies investigate access-control mechanisms such as RBAC, ABAC, DAC, MAC, and context-aware approaches [1], [8], [9], [11], [13]. These studies establish how authorization can be structured and demonstrate that increasingly distributed and context-dependent environments create additional access-control challenges. However, they do not provide a unified method for translating the resulting IAM complexity into an overall security-risk score.

Similarly, attack-graph research demonstrates that security risk can be analysed in terms of paths, dependencies, probabilities, and attacker effort [12], while scalable logical attack graphs provide techniques for analysing increasingly large security configurations [14]. These approaches provide a useful theoretical basis for representing IAM relationships as graphs, but they were not designed to provide an integrated assessment of overall cloud IAM complexity.

A further gap exists between complexity and risk. Existing literature frequently identifies complexity, excessive permissions, redundancy, policy inconsistency, privilege escalation, or

resource reachability individually. However, complexity itself should not automatically be interpreted as high risk. For example, a large IAM configuration containing many narrowly scoped and properly governed policies may be complex but secure. Conversely, a small configuration containing a wildcard permission or a short privilege-escalation path may present substantial security exposure. Paper [6] is particularly relevant to this distinction because its findings demonstrate that relatively small policies can nevertheless produce extensive resource reachability.

Therefore, the principal research gap identified by this study is:

There is no integrated and explainable theoretical model within the reviewed literature that combines measurable dimensions of cloud IAM complexity with security exposure and impact to generate a unified complexity-related IAM risk score.

The proposed research addresses this gap by synthesizing findings from IAM metrics, access-control models, policy analysis, privilege-escalation detection, and graph-based security analysis into a theoretical risk-scoring framework. Rather than treating IAM complexity as synonymous with risk, the model will seek to determine how structural, and administrative complexity interacts with security-relevant factors such as excessive privilege, privilege propagation, sensitive-resource reachability, and governance weakness.

1.7 Research Questions

RQ1: What factors contribute to complexity within cloud Identity and Access Management environments?

This question identifies the structural, policy-related, governance, contextual, and relationship-based characteristics that make cloud IAM configurations difficult to understand, maintain, and control. Relevant factors include the number of identities, roles, permissions, policies, trust relationships, policy conditions, inheritance structures, and distributed authorization dependencies.

RQ2: How does cloud IAM complexity contribute to security risk?

This question examines the relationship between complexity and security outcomes. In particular, it considers whether complexity can increase the likelihood of excessive authorization, policy misconfiguration, ineffective access reviews, unintended resource reachability, privilege accumulation, and privilege-escalation paths. The study does not assume that complexity itself is a vulnerability; instead, it investigates how complexity can act as a risk amplifier when combined with security exposure and weak governance.

RQ3: Which measurable IAM dimensions and indicators are suitable for inclusion in a theoretical cloud IAM complexity risk-scoring model?

This question identifies measurable variables from the reviewed literature that can be translated into risk dimensions. Candidate dimensions include structural complexity, policy quality and maintainability, permission exposure, privilege propagation, governance weakness, distributed or contextual complexity, and critical-resource exposure.

RQ4: How can the selected IAM complexity and security indicators be organized into an explainable theoretical risk-scoring model?

This question concerns the construction of the proposed model. It examines how individual metrics can be normalized, grouped into dimensions, weighted, and combined while maintaining interpretability. The intention is to avoid a score that functions as a black box and instead allow the overall risk assessment to be traced back to the IAM conditions that produced it.

RQ5: How can the proposed theoretical model be evaluated for coherence, coverage, explainability, and future practical applicability?

As the proposed framework is theoretical, this question focuses on evaluating whether the model adequately represents the risk factors identified in the literature, maintains logical consistency, provides sufficient coverage of the identified IAM complexity dimensions, and can be explained to security and governance stakeholders. It also considers what additional empirical validation would be required before the model could be used operationally.

1.8 Research Question Traceability Matrix

Research Question	Linked Objective	Expected Chapter / Section	Main Construct or Metric	Evaluation Metric / Evidence
RQ1: What factors contribute to complexity within cloud IAM environments?	Objective 1: Systematically review literature on cloud IAM, access control, metrics, policy verification, privilege escalation and graph-based analysis. Objective 2: Identify and classify measurable dimensions of cloud IAM complexity.	Literature Review and SLR Findings / Thematic Analysis	Structural complexity, number of identities, roles, policies, permissions, hierarchy depth, trust relationships, policy conditions, contextual attributes, governance dependencies	Number and frequency of complexity factors identified across the selected studies; thematic coverage; classification of factors into defined complexity dimensions
RQ2: How does cloud IAM complexity contribute to security risk?	Objective 3: Investigate the relationship between IAM complexity and security risk.	Literature Review, Comparative Analysis, and Discussion	Excessive privilege, misconfiguration, redundancy, ineffective access review, sensitive-resource reachability,	Evidence of relationships between complexity factors and security outcomes across the

			privilege escalation, lifecycle weaknesses	reviewed studies; identification of risk-amplifying conditions
RQ3: Which measurable IAM dimensions and indicators are suitable for inclusion in the model?	Objective 4: Evaluate existing IAM metrics and security-analysis approaches for suitability within a complexity-risk assessment.	SLR Synthesis, Model Requirements, and Model Development	Policy complexity, authorization accuracy, redundancy, maintainability, wildcard use, reachability, escalation paths, governance indicators, contextual complexity, asset criticality	Relevance of each metric to the research problem; measurability; interpretability; literature support; ability to distinguish complexity from actual security exposure
RQ4: How can the selected indicators be organized into an explainable theoretical risk-scoring model?	Objective 5: Develop a theoretical risk-scoring model. Objective 6: Define a theoretical scoring and classification mechanism.	Proposed Model / Methodology	Structural Complexity Score, Policy Quality Score, Permission Exposure Score, Privilege Propagation Score, Dynamic Complexity Score, Governance Weakness Score, Asset Criticality	Completeness of model dimensions; normalization method; weighting logic; aggregation method; traceability from overall score to contributing indicators; proposed risk bands
RQ5: How can the theoretical model be evaluated for coherence, coverage, explainability and future applicability?	Objective 7: Critically evaluate the proposed model, its assumptions, limitations, and requirements for empirical validation.	Evaluation, Discussion, and Conclusion	Model coverage, internal consistency, sensitivity, explainability, applicability, validation requirements	Coverage of literature-derived risk factors; logical consistency of scoring relationships; sensitivity of score to changes in dimensions; ability to explain score composition; identification of limitations and

				future validation requirements
--	--	--	--	--------------------------------------

The traceability matrix demonstrates that each research question is directly connected to one or more research objectives and to a defined set of measurable constructs. It also establishes where each question is addressed within the thesis and identifies the evidence that will be used to determine whether the corresponding objective has been achieved.

The matrix is particularly important for this study because the final contribution is a **theoretical model rather than a fully deployed operational system**. Accordingly, the evaluation criteria focus initially on conceptual coverage, internal coherence, literature grounding, transparency, and explainability. Empirical measures such as predictive accuracy, false-positive rate, false-negative rate, correlation with security incidents, and cross-cloud benchmarking should be identified as **future validation metrics** unless the thesis later includes a dataset or experimental implementation capable of supporting them.

Chapter 2 - Literature Review

Identity and Access Management (IAM) is a fundamental component of cloud security. It encompasses the policies, processes, technologies, and organizational responsibilities used to establish digital identities, authenticate users and services, assign permissions, and control access to cloud resources. In conventional information systems, access-control decisions were commonly associated with a limited set of users, applications, and centrally managed resources. Cloud computing has substantially expanded this environment by introducing multiple administrative domains, distributed resources, machine identities, temporary credentials, federated identities, service accounts, cross-account trust relationships, and dynamically changing workloads.

The resulting IAM configurations are increasingly difficult to understand, administer, and verify. A single effective authorization decision may depend on several interacting components, including identity policies, resource-based policies, role assignments, group memberships, permission boundaries, trust relationships, contextual conditions, and explicit deny rules. Complexity can therefore obscure excessive permissions, weaken access reviews, delay privilege revocation, and create indirect paths through which an identity can obtain access beyond its intended authority.

Existing studies examine individual aspects of this problem, including access-control models, IAM governance, policy-quality metrics, formal verification, privilege escalation, context-aware authorization, and graph-based vulnerability analysis. However, the literature does not yet provide a unified and empirically validated model for scoring the security risk created by cloud IAM complexity.

This literature review is divided thematically as follows:

1. Foundations and evolution of access-control models
2. IAM requirements and governance in cloud environments
3. complexity, quality, and maintainability
4. Misconfiguration, excessive privilege, and privilege escalation
5. Graph-based modelling of IAM and attack exposure
6. Distributed and context-aware access-control complexity

2.1 Foundations and Evolution of Access-Control Models

Access-control models define how authorization relationships are represented and how decisions concerning users, actions, and resources are made. The selected literature discusses Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Policy-Based Access Control (PBAC), Usage Control (UCON), and hybrid approaches [1], [8], [9], [11].

DAC permits resource owners to determine who may access their resources. Although flexible, DAC can become difficult to manage when permissions are delegated repeatedly or distributed across a large population of users. MAC applies centrally defined security classifications and is more restrictive, but its rigidity may limit its suitability for dynamic commercial cloud environments [1], [9]. RBAC reduces direct user-permission administration by assigning permissions to roles and assigning users to those roles. ABAC provides more fine-grained authorization by evaluating attributes associated with users, resources, requested actions, and environmental circumstances.

2.1.1 Role-Based Access Control

The NIST RBAC model provides an important theoretical foundation for modern IAM systems. It organizes access through users, roles, permissions, user-role assignments, and permission-role assignments [13]. The model distinguishes four principal forms: flat RBAC, hierarchical RBAC, constrained RBAC, and symmetric RBAC.

Flat RBAC establishes the core relationship between users, roles, and permissions. Hierarchical RBAC supports role inheritance, allowing senior roles to inherit the permissions of junior roles. Constrained RBAC introduces controls such as static and dynamic separation of duties. Symmetric RBAC adds permission-role review capabilities [13].

RBAC can simplify administration because changes to job responsibilities can be handled through role assignment rather than through direct modification of every permission. However, RBAC does not eliminate complexity. In large enterprises, organizations may create many overlapping or highly specialized roles to reflect departments, applications, locations, employment types, and exceptional responsibilities. This can produce role explosion, deep inheritance hierarchies, duplicate permission sets, and separation-of-duty conflicts.

The security implications of RBAC complexity depend on more than the number of roles. Important considerations include:

- The number of roles assigned to each identity.
- The depth of role hierarchies.
- Overlap between role permissions.
- The presence of unused or obsolete roles.
- The number of privileged roles.
- The number of inherited authorization paths.
- The effectiveness of separation-of-duty constraints.

RBAC complexity is therefore partly structural and partly organizational. A large number of clearly defined, properly governed roles may be less risky than a smaller set of broadly privileged and poorly maintained roles.

2.1.2 Attribute-Based Access Control

ABAC evaluates authorization decisions using attributes relating to subjects, objects, requested operations, and environmental conditions. It is often considered more suitable than static RBAC for dynamic cloud environments because policies can adapt to attributes such as department, device status, location, resource sensitivity, request time, and security clearance [1], [5], [8].

The flexibility of ABAC introduces a different form of complexity. Administrators must manage:

- A potentially large number of attributes.
- Attribute values from multiple authoritative sources.
- Logical conditions within policies.
- Attribute validity and update frequency.
- Policy-combining behaviour.
- Dependencies between identity, resource, and environmental attributes.

A policy containing several Boolean conditions may appear concise but may generate a large number of possible authorization states. The reliability of an ABAC decision also depends on the quality, accuracy, and timeliness of the underlying attributes. An otherwise correct policy can produce an inappropriate decision if its attribute data are outdated or inconsistent.

AWS IAM policies can be represented through a formal ABAC model based on Event Calculus. The proposed approach converts JSON-based IAM policies into a formal representation that can be analysed and verified automatically [5]. This indicates that cloud IAM authorization

cannot always be assessed reliably through manual policy inspection, particularly when multiple attributes and conditions interact.

2.1.3 Hybrid and Policy-Based Access Control

Modern cloud IAM systems rarely implement a single access-control model in isolation. They commonly combine role assignments, identity attributes, resource-specific policies, trust relationships, organization-wide restrictions, and contextual conditions. Major access-control families as DAC, MAC, RBAC, ABAC, and PBAC, while emphasizing that different models address different technical, organizational, and business requirements [9].

A hybrid model can provide greater flexibility and finer-grained control. Nevertheless, it can also create policy interactions that are difficult to understand. An authorization may be allowed by an identity policy, limited by a permission boundary, affected by a resource policy, and ultimately denied by a higher-level organizational control. The effective permission is therefore not necessarily visible in any single policy document.

Effective access-control policies should demonstrate consistency, relevance, minimality, completeness, and correctness [9]. A policy is consistent when its permission and denial rules do not produce unintended contradictions. It is relevant when its rules correspond to actual activities, minimal when unnecessary and reducible rules are removed, complete when relevant actions are covered, and correct when its behaviour aligns with intended requirements [9].

These properties demonstrate that IAM complexity must be evaluated in relation to policy interaction and quality rather than solely through the number of policy statements.

2.2. IAM Requirements and Governance in Cloud Environments

Cloud IAM is broader than technical policy enforcement. It includes identity creation, authentication, authorization, access certification, lifecycle management, regulatory compliance, segregation of duties, monitoring, and removal of access when it is no longer required.

Identity and access management mechanisms and challenges in cloud environments [2]. It identifies authentication, authorization, access-control governance, certification, risk scoring, lifecycle management, and segregation of duties as important components of cloud IAM [2]. Its treatment of certification and risk scoring establishes that access decisions must be assessed continuously rather than treated as one-time administrative actions.

Cloud IAM must manage both human and non-human identities. Human identities include employees, contractors, customers, administrators, and external partners. Non-human identities include applications, virtual machines, containers, serverless functions, automated processes, and cloud services. Non-human identities are particularly significant because they may operate continuously, hold persistent credentials, or obtain permissions through role-assumption mechanisms.

2.2.1 Enterprise IAM Requirements

Enterprise IAM requirements are divided into four categories [4]:

- Security and compliance
- Operability
- Technology
- User requirements

Security and compliance requirements include appropriate authentication, least privilege, access monitoring, regulatory conformity, and protection against unauthorized access. Operability requirements concern manageability, scalability, automation, reliability, and integration with business processes. Technology requirements include compatibility, interoperability, performance, and support for heterogeneous infrastructures. User requirements relate to usability, convenience, transparency, and the reduction of authentication burden [4].

These categories are interdependent. A highly restrictive system may improve one dimension of security but reduce usability and operational efficiency. Conversely, simplified access procedures may improve user experience while weakening control. IAM risk scoring must therefore recognize that IAM quality is not represented by a single security measure.

It also evaluates the potential contribution of Self-Sovereign Identity (SSI) [4]. SSI may improve authentication, manageability, user control, and selected least-privilege practices. However, the study concludes that SSI is not a complete solution to the challenges of enterprise IAM [4]. This finding is relevant because technological innovation alone does not remove the organizational and authorization complexity associated with enterprise access.

2.2.2 Identity Lifecycle Complexity

Identity lifecycle management commonly includes joiner, mover, and leaver processes. When a person joins an organization, an identity and initial access rights are created. When the person changes position, existing rights should be reviewed and adjusted. When the person leaves, access should be removed promptly.

IAM must interact with business events such as joining an organization, changing departmental affiliation, leaving the organization, and onboarding applications. As organizations increase in scale, these activities require specialized IAM technologies and processes [3].

Failures in identity lifecycle management can produce:

- Orphaned accounts
- Dormant accounts
- Retained permissions after role changes
- Excessive cumulative access
- Inactive but privileged service identities
- Delayed revocation

- Unclear ownership of accounts or policies

These weaknesses may develop gradually. An employee can accumulate permissions through multiple role changes without losing permissions from previous responsibilities. This form of privilege accumulation can be difficult to identify when permissions are inherited indirectly or distributed across multiple cloud platforms.

2.2.3 Access Reviews and Governance Burden

Access reviews are intended to confirm that assigned privileges remain appropriate. However, the effectiveness of a review depends on whether reviewers understand the policies, resources, roles, and business consequences involved. A technically complete review may provide little security value when reviewers approve permissions without sufficient analysis.

IAM goals can conflict [3]. Access reviews support compliance but require time and domain expertise. Under operational pressure, reviewers may approve authorizations quickly rather than evaluate whether they remain necessary. This may satisfy a formal compliance requirement while failing to reduce security risk [3].

This finding links IAM complexity directly to governance quality. As the number of identities, roles, permissions, and resources increases, the cognitive burden placed on reviewers also increases. Complexity can therefore reduce the effectiveness of controls that technically ex

2.3. IAM Metrics, Policy Complexity, and Policy Quality

The development of a theoretical risk-scoring model requires measurable variables. According to [3], it provides the most direct contribution to this requirement by systematically reviewing IAM metrics. It identifies 43 metrics across seven perspectives and connects them with IAM objectives such as security, compliance, operational efficiency, process quality, and cost [3].

The study emphasizes that IAM terminology remains inconsistent and that no universally accepted collection of IAM metrics has been established. It recommends standardized terminology, process-specific metric sets, and IAM maturity models supported by quantifiable benchmarks [3].

2.3.1 Authorization Accuracy

Authorization accuracy concerns the extent to which granted and denied permissions correspond to legitimate business requirements. Paper [3] identifies two principal authorization errors:

- Excessive authorizations.
- Missing authorizations.

Excessive authorizations grant more access than is necessary and increase security risk. Missing authorizations deny required access and can disrupt operations [3].

This distinction is important for risk scoring. A model based only on the number of permissions may misclassify legitimate access as risky. Risk assessment requires comparison with an

expected or approved authorization baseline. Establishing that baseline is difficult because it requires detailed knowledge of users' responsibilities, the meaning of permissions, and internal security requirements.

The two types of error may be represented conceptually using classification terminology:

- A correctly granted authorization is a true positive.
- A correctly denied authorization is a true negative.
- An excessive authorization is a false positive.
- A missing authorization is a false negative.

From a cybersecurity perspective, excessive authorizations may receive a higher risk weighting because they can directly enable unauthorized actions. Missing authorizations remain important because they can create operational workarounds, emergency privileges, and pressure to introduce broad exceptions.

2.3.2 Policy Complexity

Paper [3] treats complexity as a policy-quality metric associated with maintainability. Lower policy complexity can reduce administrative cost and support better long-term policy quality. Complexity is also used in role-mining research to evaluate candidate role structures [3].

Potential indicators of policy complexity include:

- Number of policies.
- Number of policy statements.
- Number of actions.
- Number of resources.
- Number of conditions.
- Number of attributes.
- Number of policy layers.
- Number of references to external roles or policies.
- Depth of nested logical expressions.
- Number of interacting allow and deny rules.

However, policy size should not be treated as equivalent to risk. A short policy containing wildcard access may be more dangerous than a long but narrowly scoped policy. Complexity measures must therefore be combined with exposure and impact measures.

2.3.3 Redundancy

Redundancy occurs when the same authorization is granted through multiple roles, groups, or policies. Paper [3] associates redundancy with maintenance errors, confusion, and ineffective revocation. A permission may appear to have been removed from one policy while continuing to apply through another relationship [3].

In cloud IAM, redundancy may arise when:

- The same permission is assigned directly and through a group.
- Multiple roles contain overlapping permissions.
- A managed policy and an inline policy grant the same action.
- Permissions are inherited through several trust relationships.
- Similar policies are copied across multiple accounts.

Redundancy does not necessarily indicate immediate exposure, but it increases the probability of administration errors and makes effective access more difficult to determine.

2.3.4 Understandability and Maintainability

Policy understandability refers to the ability of administrators, reviewers, and governance personnel to determine what a policy means and what access it creates. Maintainability concerns the ease with which policies can be updated while preserving correctness.

Paper [3] describes maintainability as being influenced by understandability, complexity, redundancy, automation, and policy-attribute quality [3].

A policy may be technically valid but difficult for a human reviewer to interpret. Understandability may be weakened by:

- Ambiguous names.
- Missing descriptions.
- Absent policy owners.
- Deeply nested conditions.
- Large numbers of indirect assignments.
- Inconsistent policy structures.
- Interactions across cloud accounts.
- Provider-specific terminology.

This presents an important theoretical relationship:

As IAM complexity increases, human understanding and maintenance accuracy may decrease, thereby increasing the probability that security weaknesses remain undetected.

2.3.5 Automation

Automation can reduce the manual burden of updating access rights. ABAC can automatically reflect organizational changes when authoritative attribute values are updated. RBAC systems may use automated provisioning workflows to update role assignments.

Nevertheless, Paper [3] notes that automation cannot eliminate maintenance because automated processes have limited scope and may operate on inaccurate or outdated policies [3].

Automation may therefore reduce operational complexity while introducing dependence on:

- Attribute accuracy.
- Workflow correctness.
- Synchronization.
- Integration reliability.
- Rule quality.
- Exception handling.

A risk model should not interpret greater automation as automatically producing lower risk. The quality and coverage of automation must also be evaluated.

2.4 IAM Misconfiguration, Excessive Privilege, and Privilege Escalation

Cloud IAM misconfiguration occurs when an access-control configuration does not enforce the intended security requirements. Misconfiguration may create overly broad permissions, unintended trust relationships, publicly accessible resources, ineffective denial rules, or paths through which privileges can be increased.

Paper [6] identifies IAM policy misconfiguration as a significant problem in serverless computing. Serverless applications can contain many functions, services, and resources, each of which may act as a security principal. This increases the difficulty of implementing least-privilege policies [6].

2.4.1 Excessive Permission

Excessive permission exists when an identity possesses access beyond what is necessary for its intended responsibilities. It may result from:

- Wildcard actions.
- Wildcard resources.
- Broad managed policies.
- Excessive role membership.

- Outdated permissions.
- Unnecessary trust relationships.
- Inherited privileges.
- Copied default policies.

Excessive privilege increases the potential impact of compromised credentials. An attacker who compromises a narrowly privileged account may have limited options, whereas compromise of an overprivileged identity may provide access to sensitive data, administrative actions, or additional identities.

Paper [6] reports that serverless policies can be short yet highly permissive. In its analysed corpus of 731 open-source AWS Lambda applications, 92% of the policies consisted of no more than ten statements, while 30% permitted full reachability between application functions and resources [6]. This demonstrates that statement count alone is an inadequate indicator of risk.

2.4.2 Privilege Escalation

Privilege escalation occurs when an attacker or untrusted identity obtains permissions beyond those initially assigned. Paper [7] identifies IAM misconfiguration as a major cause of privilege-escalation attacks. It conceptualizes IAM configurations as relationships among users, groups, roles, services, and permissions [7].

Permissions may be obtained directly or inherited through entity relationships. For example, a user may receive permissions through group membership, assume a role with additional access, or use one service permission to modify another IAM entity. Paper [7] represents these relationships as a multi-relational graph in which nodes represent entities and permissions and edges represent assignments and associations [7].

The study identifies five categories of privilege escalation that share a common principle: permissions propagate between entities. It extracts 219 permission-flow templates and constructs a benchmark containing 2,500 tasks designed to reflect the scale and diversity of real IAM configurations [7].

This work indicates that privilege risk cannot always be identified by inspecting an identity's current permissions. Assessment must also consider what permissions the identity could acquire through allowed actions and relationships.

2.4.3 Limitations of Existing Detection Approaches

Paper [7] identifies two major limitations in existing privilege-escalation detection tools. First, individual tools cover only subsets of possible escalation types. Second, many tools require complete access to IAM configuration data [7].

The requirement for full configuration visibility creates practical difficulties for external security providers and organizations that are reluctant to disclose sensitive infrastructure

details. Partial visibility may also occur within large enterprises when different teams control different cloud accounts or platforms.

This suggests that an IAM risk-scoring model should account for **assessment confidence**. A low reported risk score based on incomplete configuration data may not accurately represent the real environment.

2.5 Formal Verification of IAM Policies

Formal verification applies mathematically defined models to determine whether policies satisfy specified properties. Paper [5] develops an Event Calculus-based ABAC model for AWS IAM policies. The framework automatically converts JSON policies into a formal representation and evaluates the approach using actual IAM policies [5].

Formal methods can identify:

- Contradictory rules.
- Unintended permission combinations.
- Policy inconsistency.
- Unreachable rules.
- Ineffective restrictions.
- Deviations from specified security properties.

The principal strength of formal verification is that it evaluates policy logic systematically. Manual examination becomes unreliable when policies contain many conditions, exceptions, and interacting layers.

However, formal verification depends on the correctness of the security properties against which a policy is assessed. A policy may be formally consistent but still violate the principle of least privilege if its specified requirements permit excessive access. Formal verification therefore supports but does not replace organizational risk assessment.

For a theoretical IAM complexity-risk model, formal verification results may be used as indicators such as:

- Number of policy conflicts.
- Number of failed security properties.
- Number of unreachable rules.
- Number of unintended authorization combinations.
- Verification coverage.

2.6 Graph-Based Modelling of IAM Complexity and Risk

Graph-based analysis is particularly relevant to cloud IAM because IAM configurations consist of interconnected entities and relationships. A graph can represent identities, groups, roles, services, permissions, and resources as nodes, while edges represent membership, assignment, trust, access, and role-assumption relationships.

Graph analysis supports the identification of:

- Direct permissions.
- Inherited permissions.
- Reachable resources.
- Privilege-escalation paths.
- Highly connected roles.
- Single points of privilege concentration.
- Attack paths.
- Indirect trust relationships.

2.6.1 Reachability Analysis

Paper [6] introduces Grasp, a graph-based framework for analysing serverless IAM policies. Grasp transforms application specifications and policies into reachability graphs that show permitted interactions among principals and resources [6].

The graphs can be queried to determine:

- Whether a public function can access a private resource.
- Whether one function can invoke another.
- Whether a resource is accessible to an unintended principal.
- Whether a path exists from an exposed component to sensitive data.

This approach provides more meaningful security information than policy-size metrics because it evaluates the effective consequences of policy relationships.

A reachability-based IAM measure could consider:

- Number of sensitive resources reachable by untrusted identities.
- Number of public-to-private access paths.
- Path length.
- Number of intermediary roles or services.
- Criticality of reachable resources.

- Actions available at the destination.

2.6.2 Network Vulnerability and Attack Graphs

Paper [12] presents a graph-based system for network-vulnerability analysis. The system represents attack stages as nodes and attacks or transitions as edges. Probabilities or attacker-effort costs can be assigned to edges, allowing algorithms to identify high-probability or low-effort paths [12].

Although the work focuses on network vulnerabilities rather than cloud IAM specifically, its principles are applicable to IAM. An IAM privilege path may be represented as a sequence in which an attacker:

1. Compromises an identity.
2. Uses an assigned permission.
3. Assumes another role.
4. Modifies a policy.
5. Obtains access to a sensitive resource.

Paper [12] also discusses the limitations of relying solely on the shortest path or total path count. It considers Mean Effort to Failure and argues that a set of near-optimal paths may provide a more informative measure of security [12].

For IAM risk analysis, this means that one short privilege-escalation path may be critical, but multiple slightly longer paths may also indicate substantial systemic exposure.

2.6.3 Scalable Attack-Graph Generation

A major limitation of graph-based security assessment is computational scalability. As the number of entities and relationships grows, the number of possible paths can increase rapidly.

Paper [14] proposes logical attack graphs that represent dependencies among attack goals and configuration information. The approach is based on MulVAL and produces graphs whose size is polynomial relative to the analysed network. The authors report quadratic-time graph generation and substantial scalability improvements over earlier approaches [14].

This work is important for cloud IAM because enterprise environments can contain thousands of identities, roles, services, and resources. A theoretically valid risk-scoring model has limited practical value if its underlying analysis cannot scale to realistic configurations.

2.6.4 Graph Complexity as a Risk Indicator

Graph-based IAM complexity may be measured using:

- Number of nodes.
- Number of edges.
- Graph density.

- Average node degree.
- Maximum node degree.
- Hierarchy depth.
- Number of cycles.
- Number of privilege paths.
- Shortest path to critical resources.
- Centrality of privileged roles.
- Number of externally reachable nodes.

However, high graph density is not automatically equivalent to high security risk. A dense graph may contain many legitimate low-impact relationships. Graph metrics should therefore be weighted according to permission severity, resource sensitivity, external exposure, and the effort required to traverse a path.

2.7 Distributed, Fog, and Context-Aware Access-Control Complexity

Cloud services increasingly interact with fog computing, edge platforms, IoT devices, blockchain networks, and software-defined networking. These environments extend IAM decisions across multiple systems and administrative domains [8]-[11].

Paper [9] reviews access control across cloud, blockchain, IoT, and software-defined networking. It highlights the need to integrate access-control technologies with broader cybersecurity and network-architecture strategies [9]. Access control in distributed environments must function despite differences in system architecture, trust assumptions, device capabilities, and administrative ownership.

2.7.1 Distributed Authorization

Paper [10] explains that distributed systems require authentication and authorization capabilities comparable to conventional systems. However, authorization becomes more difficult because privileges must be coordinated across independent systems. Poorly designed controls may either restrict legitimate sharing excessively or allow data to be shared too permissively [10].

Distributed IAM complexity can arise from:

- Multiple identity providers.
- Cross-domain trust.
- Inconsistent policy models.
- Delayed synchronization.
- Duplicated identities.

- Conflicting authorization rules.
- Fragmented ownership.
- Incomplete visibility.

A risk-scoring model should therefore consider the number of trust domains and the degree to which permissions are synchronized and consistently enforced.

2.7.2 Fog Computing

Fog computing moves selected computation and storage closer to users and IoT devices. This can reduce latency and bandwidth requirements but introduces additional access-control challenges.

Paper [11] identifies access control as a fundamental security requirement in fog computing. Fog systems may process personal information and involve users, fog providers, and cloud providers that do not fully trust one another [11].

Relevant complexity factors include:

- Geographical distribution.
- Device mobility.
- Limited computing resources.
- Low-latency authorization requirements.
- Temporary connections.
- Interaction between fog and cloud layers.
- Heterogeneous devices.
- Multiple service providers.

These characteristics make centralized, static access-control decisions less effective.

2.7.3 Context-Aware Access Control

Paper [8] reviews context-aware access control for cloud and fog networks. Contextual information may include:

- Location.
- Request time.
- User profile.
- Relationship type.
- Relationship strength.
- Purpose of access.

- Situational conditions [8].

The study proposes fog-based context-aware access control that moves some policy logic from centralized cloud systems to intermediary edge nodes [8].

Context-aware authorization can improve security because access decisions adapt to the circumstances of a request. Nevertheless, it increases the number of variables and possible authorization outcomes. Context data may also be inaccurate, missing, manipulated, or delayed.

The complexity created by context-aware access control may therefore depend on:

- Number of contextual attributes.
- Number of context sources.
- Rate of contextual change.
- Number of conditional rules.
- Reliability of context information.
- Interaction between contextual conditions.
- Frequency of policy re-evaluation.

2.8 Synthesis of the Literature

The reviewed studies demonstrate that cloud IAM complexity has several dimensions.

2.8.1 Structural Complexity

Structural complexity concerns the size and interconnectedness of the IAM configuration. It includes the number of identities, roles, groups, permissions, policies, resources, conditions, and trust relationships.

Structural complexity increases the amount of information that administrators and tools must process. However, size alone does not establish security risk.

2.8.2 Logical Complexity

Logical complexity concerns the interactions among policy rules, conditions, allows, denies, inheritance relationships, and access-control models. A small number of policies may have high logical complexity when their effects depend on several external conditions or policy layers.

2.8.3 Administrative Complexity

Administrative complexity concerns the effort required to provision, review, modify, and revoke access. It is influenced by redundancy, role overlap, unclear ownership, lifecycle delays, and manual processes.

2.8.4 Dynamic Complexity

Dynamic complexity arises when authorization depends on frequently changing attributes, temporary credentials, role assumptions, context, or distributed-system state.

2.8.5 Exposure Complexity

Exposure complexity concerns the number and severity of paths through which identities can reach permissions or resources. It includes inherited access, privilege escalation, public-to-private paths, and cross-account trust chains.

The literature indicates that these dimensions are related but should not be treated as interchangeable. For example:

- A large configuration can be well governed and low risk;
- A small configuration can contain unrestricted permissions;
- A formally consistent policy can still grant excessive access;
- A user with limited direct permissions may possess a serious privilege-escalation path;
- Automated provisioning can reduce administrative workload but propagate incorrect access at scale.

Cloud IAM complexity should therefore be treated as a risk-amplifying condition, not as a vulnerability in isolation. It increases the probability that policy defects, excessive permissions, and escalation paths will be introduced or remain undetected.

2.8.6 Comparative Analysis of Reviewed Studies

Study	Approach	Domain	Metrics	Key Limitation	How the proposed model differs
1	Comparative survey of access-control mechanisms	Cloud access control	Scalability, flexibility, security, fine-grained control, delegation, auditability, maintainability, trust	Compares access-control models rather than quantifying the security risk arising from IAM complexity	Converts characteristics of access-control complexity into components of an integrated IAM risk-scoring framework
2	Survey/taxonomy of cloud IAM mechanisms and challenges	Cloud IAM	Authentication, authorization, credentials, access governance, certification, risk score, lifecycle management, segregation of duties	Broad IAM review; does not provide an integrated quantitative	Incorporates governance and lifecycle weaknesses alongside technical IAM complexity and exposure

				complexity -risk model	
3	Systematic review and synthesis of IAM metrics	Enterprise IAM measurement	43 IAM metrics across seven perspectives; includes authorization accuracy, complexity, redundancy, maintainability, security, process and software quality	Provides a broad metric catalogue but does not define detailed formulas for individual metrics or combine them into a cloud IAM complexity-risk score	Selects complexity-relevant measures and organizes them into risk dimensions that can ultimately contribute to an overall score
4	Systematic review of enterprise IAM requirements and assessment of SSI contributions	Enterprise IAM / Self-Sovereign Identity	Security and compliance, operability, technology, user requirements, manageability, usability, least privilege	Requirement-oriented rather than designed to quantify IAM configuration on risk	Uses governance and operational requirements as risk-relevant dimensions while concentrating specifically on cloud IAM complexity
5	Formal ABAC representation and policy verification using Event Calculus	AWS IAM policy verification	Policy rules, attributes, authorization behaviour and verification properties	Focuses on logical verification of policies; does not measure overall IAM complexity, governance or attack exposure	Treats policy correctness as one component of a wider model incorporating complexity, exposure, propagation and governance
6	Grasp reachability-graph analysis	AWS Lambda / serverless IAM	Policy reachability, public accessibility, direct and indirect access paths, read/write paths, connectivity and excessive privilege	Primarily serverless/AWS focused; incomplete configuration information	Extends the concept of reachability beyond serverless policy analysis by treating exposure/reach

				n can produce incomplete graphs, and it does not generate an overall IAM complexity -risk score	ability as one dimension of broader IAM complexity risk
7	TAC hybrid privilege-escalation detection using permission-flow graphs; white-box and grey-box analysis	AWS IAM privilege escalation	Five PE categories, 219 permission-flow templates, entity relationships, permission propagation, PE coverage and graph-based relationships	Primarily detects privilege escalation and currently targets AWS; it does not evaluate broader IAM complexity or governance	Uses privilege propagation/escalation as a risk dimension rather than treating PE detection as the complete IAM risk assessment
8	Survey/taxonomy of context-aware access-control mechanisms	Cloud, fog and IoT access control	Location, time, profile, relationship, purpose, situational and other contextual conditions	Concentrates on context-aware authorization rather than measuring aggregate IAM complexity risk	Incorporates contextual dynamism as a complexity dimension alongside policies, permissions, governance and attack exposure
9	Survey and comparative analysis of access-control techniques	Cloud, blockchain, IoT and SDN	DAC, MAC, RBAC, ABAC and PBAC; policy consistency, relevance, minimality, completeness and correctness	Broad cross-domain survey; does not translate policy-quality characteristics into a unified IAM risk score	Uses relevant policy-quality characteristics as measurable contributors to complexity-related cloud IAM risk

10	Analysis of access-control requirements for emerging distributed systems	Distributed systems	Authentication, authorization, privilege coordination/synchronization and distributed policy requirements	Addresses distributed authorization challenges conceptually rather than providing a quantitative IAM complexity model	Incorporates cross-domain relationships and distributed authorization complexity into a structured risk model
11	Survey/classification of fog access-control approaches	Fog computing	Distribution, mobility, cloud interaction, trust, resource constraints and access-control requirements	Specific to fog-computing access control and does not quantify IAM complexity as an overall risk	Generalizes relevant distributed and dynamic complexity factors into cloud IAM risk dimensions
12	Graph-based network-vulnerability analysis	Network security	Attack paths, attack success probability, attacker effort/cost, shortest paths, Mean Effort to Failure and near-optimal paths	Designed for network vulnerabilities rather than IAM entities, [1] policies and governance	Adapts path-based risk reasoning to IAM relationships, particularly privilege propagation and access to critical cloud resources
13	NIST RBAC reference model	Role-based access control	Users, roles, permissions, role hierarchies, constraints, user-role and permission-role relationships	Standardizes RBAC but is not a risk-assessment or complexity-scoring model	Treats role structure, hierarchy and relationships as potential structural-complexity indicators within a broader IAM risk model
14	Logical attack-graph generation /	Network attack modelling	Attack dependencies, attack paths, configuration	Focuses on scalable generation of network	Applies the underlying concept of scalable

	MulVAL-based analysis		relationships and graph scalability	attack graphs rather than cloud IAM complexity or governance	dependency/path analysis to IAM while integrating it with policy, governance and permission-risk dimensions
Proposed study	Theoretical Cloud IAM Complexity Risk-Scoring Model	Cloud IAM	Structural complexity, policy quality and maintainability, permission exposure, privilege propagation/escalation, contextual/distributed complexity, governance weakness and critical-resource exposure	Theoretical model requires subsequent empirical validation, calibration of weights and testing of thresholds	Integrates previously separated IAM complexity, quality, governance, privilege and graph-exposure factors into one explainable theoretical risk-scoring framework

Chapter 3 - Methodology

3.1 Research Design

This study adopts a theoretical, literature-based research design to develop an explainable risk-scoring model for cloud Identity and Access Management (IAM) complexity. Following the Saunders Research Onion, the study adopts a Positivist research philosophy, a Deductive approach, and Design Science Research (DSR) as the research strategy, based on Hevner et al. (2004), with a Systematic Literature Review (SLR) used as the underlying synthesis method.

The methodology follows the four research objectives: Review, Analyse, Build, and Evaluate. The research does not deploy or empirically validate an operational IAM system; instead, it synthesizes findings from existing research to identify measurable complexity and security factors and organize them into a theoretical risk-scoring framework.

3.2 Literature Review and Data Extraction

The study uses selected academic papers forming the research corpus. These studies cover cloud IAM, access-control models, IAM metrics, governance, policy verification, privilege escalation, distributed authorization, context-aware access control, reachability analysis, and attack graphs.

Relevant information was extracted from each study according to:

- Research approach and domain.
- IAM complexity factors.
- Security-risk factors.
- Proposed metrics or measurable indicators.
- Limitations.
- Relevance to the proposed model.

The findings were analysed thematically to identify recurring relationships between IAM complexity and security exposure.

3.3 Identification of Model Dimensions

The thematic analysis was used to consolidate related factors into seven model dimensions:

- Structural Complexity (SC).
- Policy Quality and Maintainability Weakness (PQ).
- Permission Exposure (PE).
- Privilege Propagation (PP).
- Dynamic and Contextual Complexity (DC).
- Governance Weakness (GW).
- Asset Criticality (AC).

These dimensions reflect the main areas identified across the reviewed literature, including policy complexity and maintainability, excessive authorization, privilege escalation, governance weaknesses, contextual dependencies, and graph-based resource reachability.

3.4 Model Development

The selected indicators are normalized to a common scale from 0 to 1, where higher values represent greater complexity or risk. Indicators are combined into their respective dimensions before being grouped into two principal components:

$$C = \frac{SC + PQ + DC + GW}{4}$$

where C represents the **Complexity Component**, and:

$$E = \frac{PE + PP}{2}$$

where E represents the Exposure Component.

The complete scoring mechanism, weighting assumptions, interaction between complexity and exposure, asset criticality adjustment, and risk classifications are presented in the Proposed Cloud IAM Complexity Risk-Scoring Model chapter.

Equal weighting is initially used because the reviewed literature does not provide sufficient empirical evidence to justify precise differential weights. The weighting and thresholds are therefore treated as theoretical and provisional.

3.5 Model Evaluation

Because the proposed model is theoretical, evaluation focuses on conceptual validity rather than predictive accuracy. The model is assessed according to:

- Literature coverage.
- Logical coherence.
- Traceability.
- Explainability.
- Measurability.
- Distinctiveness from existing approaches.
- Potential applicability to cloud IAM environments.

A worked hypothetical example and sensitivity of the score to changes in individual dimensions are used to demonstrate how the model operates and how the final result can be traced to its underlying factors.

3.6 Limitations and Validity

The principal limitation is that the model is derived from a relatively small literature corpus and has not yet been validated using operational cloud IAM data. The reviewed studies also contain a strong AWS representation, particularly in privilege-escalation and reachability research.

Chapter 4 - Proposed Cloud IAM Complexity Risk-Scoring Model

4.1 Model Overview

The proposed Cloud IAM Complexity Risk Score (CICRS) is designed to assess the security risk associated with complexity in cloud Identity and Access Management environments. The model does not assume that complexity alone represents insecurity. Instead, it treats complexity as a risk-amplifying condition whose significance increases when it is combined with excessive permissions, indirect privilege propagation, weak governance, and exposure of critical resources.

The model is based on three conceptual components:

$$\text{Complexity} + \text{Security Exposure} + \text{Interaction}$$

These components are then adjusted according to the criticality of the affected cloud assets.

The model therefore distinguishes between:

- **Complexity:** how difficult an IAM environment is to understand, administer, and maintain.
- **Exposure:** what an identity can access directly or indirectly.
- **Impact:** the importance or sensitivity of the resources potentially affected.

This distinction is supported by [6], which demonstrates that relatively small IAM policies can still produce extensive resource reachability, indicating that policy size alone is not a sufficient measure of security risk.

4.2 Final Risk Dimensions

Seven dimensions are included in the proposed model.

Code	Risk Dimension	Example Indicators	Rationale
SC	Structural Complexity	Roles per identity, policy count, hierarchy depth, trust relationships, graph density	Large and highly interconnected IAM structures increase administrative and reasoning difficulty [5], [13].
PQ	Policy Quality and Maintainability Weakness	Redundancy, conflicts, wildcard use, nested conditions, unowned policies	Poor-quality and redundant policies reduce understandability and maintainability [3], [9].
PE	Permission Exposure	Excessive permissions, privileged access, public	Broad permissions increase the potential impact of identity compromise [3], [6].

Code	Risk Dimension	Example Indicators	Rationale
		access, sensitive-resource reachability	
PP	Privilege Propagation	Escalation paths, inherited permissions, role-assumption chains, shortest path to privilege	Effective privilege may exceed directly assigned privilege because permissions propagate through IAM relationships [7].
DC	Dynamic Contextual Complexity and	Context attributes, trust domains, policy updates, synchronization dependencies	Dynamic and distributed authorization introduces additional states and decision dependencies [8], [10], [11].
GW	Governance Weakness	Dormant accounts, overdue reviews, orphaned identities, revocation delay, SoD conflicts	Weak governance allows inappropriate permissions to persist even when technical controls exist [2]-[4].
AC	Asset Criticality	Data sensitivity, administrative capability, regulatory importance, business criticality	Identical IAM weaknesses do not create identical risk when the affected assets have different business or security importance.

The four complexity-related dimensions, *SC*, *PQ*, *DC*, and *GW*, describe how difficult the IAM environment is to administer reliably. The two exposure dimensions, *PE* and *PP*, measure the security consequences that can result from the configuration. *AC* represents the potential impact of those consequences.

4.3 Indicators and Metrics

4.3.1 Structural Complexity

Structural complexity represents the size and interconnectedness of the IAM configuration.

Possible indicators include:

- SC_1 = Average roles per identity
- SC_2 = Role hierarchy depth
- SC_3 = Policy-to-identity ratio
- SC_4 = Number of trust relationships
- SC_5 = IAM graph density

These indicators are included because cloud IAM permissions may be distributed through roles, groups, inheritance, and trust relationships. RBAC provides administrative benefits, but increasingly complex role structures can lead to role explosion and difficult-to-maintain relationships [5], [13].

4.3.2 Policy Quality and Maintainability Weakness

This dimension evaluates whether IAM policies are difficult to understand, inconsistent, or unnecessarily complex.

Potential indicators include:

- PQ_1 = Policy redundancy rate
- PQ_2 = Policy conflict rate
- PQ_3 = Wildcard permission ratio
- PQ_4 = Percentage of unowned policies
- PQ_5 = Average conditional complexity

Policy complexity, redundancy, authorization quality, and maintainability are explicitly identified as relevant IAM metrics in [3]. Policy consistency, minimality, completeness, and correctness are also highlighted in [9].

4.3.3 Permission Exposure

Permission exposure represents the extent to which existing permissions create direct security exposure.

Possible indicators include:

- PE_1 = Excessive permission rate
- PE_2 = Privileged identity ratio
- PE_3 = Sensitive-resource reachability
- PE_4 = Public or external accessibility
- PE_5 = Critical-action availability

This dimension is separated from structural complexity because an environment can be structurally simple but highly permissive. Grasp [6], for example, found that short policies could still permit extensive connectivity between serverless functions and resources.

4.3.4 Privilege Propagation

Privilege propagation measures permissions that can be obtained indirectly.

Potential indicators include:

- PP_1 = Number of privilege-escalation paths
- PP_2 = Shortest escalation-path length
- PP_3 = Maximum inheritance depth
- PP_4 = Number of cross-role or cross-account chains
- PP_5 = Severity of obtainable privilege

Paper [7] demonstrates that IAM privilege escalation can be represented as permission flows between entities. Therefore, assessing only the permissions currently assigned to an identity would underestimate the risk created by permissions that can subsequently be obtained.

Graph-based approaches in [12] and [14] further support the use of path length, dependencies, and reachable states when assessing security exposure.

4.3.5 Dynamic and Contextual Complexity

Dynamic complexity captures authorization conditions that change according to environmental or contextual information.

Indicators may include:

- DC_1 = Number of contextual attributes
- DC_2 = Number of context sources
- DC_3 = Number of administrative/trust domains
- DC_4 = Policy or attribute change frequency
- DC_5 = Permission synchronization delay

Context-aware access control may depend on location, time, user attributes, relationships, purpose, and situational conditions [8]. Distributed and fog environments add additional synchronization, trust, and administrative dependencies [10], [11].

4.3.6 Governance Weakness

Governance weakness measures deficiencies in the processes used to maintain IAM configurations.

Possible indicators include:

- GW_1 = Dormant account rate
- GW_2 = Orphaned identity rate
- GW_3 = Overdue access-review rate
- GW_4 = Average revocation delay
- GW_5 = Segregation-of-duty conflict rate

Governance is included because IAM security depends not only on policy design but also on lifecycle management, certification, ownership, access reviews, and segregation of duties [2]-[4].

4.3.7 Asset Criticality

Asset criticality represents the impact associated with successful unauthorized access.

A simple four-level classification is proposed:

Asset Category	Normalized Criticality
Low	0.25
Moderate	0.50
High	0.75
Critical	1.00

Criticality may be determined from factors such as:

- Sensitivity of stored data.
- Administrative capability.
- Regulatory requirements.
- Financial importance.
- Operational importance.

Where multiple assets are affected, the highest criticality value may be used when assessing a specific IAM attack or privilege path.

4.4 Metric Normalization

The proposed metrics use different measurement units. For example, hierarchy depth may be an integer, redundancy may be a percentage, and access-review delay may be measured in days. Therefore, all indicators must be transformed onto a common scale:

$$0 \leq x_i \leq 1$$

where:

- 0 represents the lowest complexity or risk condition.
- 1 represents the highest defined condition.

For indicators where a **higher value represents greater risk**, threshold-based normalization is proposed:

$$x_i = \min\left(\frac{X_i}{T_i}, 1\right)$$

where:

- X_i = observed value;
- T_i = defined high-risk threshold.

For example, if ten wildcard policies are defined as the upper threshold and an environment contains six:

$$x_i = \frac{6}{10} = 0.60$$

For indicators where a higher value represents better security, the normalized value can be inverted:

$$x_i = 1 - \min\left(\frac{X_i}{T_i}, 1\right)$$

This ensures that all normalized indicators follow the same interpretation:

Higher value = higher risk.

The thresholds are theoretical in the initial model and would require empirical calibration in future work.

4.5 Dimension Scoring

Each risk dimension is calculated from its normalized indicators.

For dimension D :

$$D = \sum_{i=1}^n w_i x_i$$

where:

- x_i is the normalized indicator;
- w_i is the indicator weight;
- $\sum w_i = 1$.

For the initial theoretical model, equal weighting is recommended.

For example, where Structural Complexity contains five indicators:

$$SC = \frac{SC_1 + SC_2 + SC_3 + SC_4 + SC_5}{5}$$

Equal weighting is appropriate at this stage because the reviewed literature does not provide sufficient empirical evidence to demonstrate that one indicator should have a specific numerical priority over another.

Future research could calibrate these weights through:

- Expert elicitation.
- Analytic Hierarchy Process (AHP)
- Historical IAM incident data.

- Statistical regression.
- Machine-learning approaches.

4.6 Complexity and Exposure Components

The six primary dimensions are divided into two higher-level components.

Complexity Component:

$$C = \frac{SC + PQ + DC + GW}{4}$$

This represents the difficulty of understanding, maintaining, and governing the IAM environment.

Exposure Component:

$$E = \frac{PE + PP}{2}$$

This represents the direct and indirect security exposure created by existing permissions.

Separating these components prevents the model from assuming that a complex system is necessarily insecure.

4.7 Final Cloud IAM Complexity Risk Score

The proposed final score is:

$$CICRS = 100 \times AC \times \frac{C + E + (C \times E)}{3}$$

where:

- $CICRS$ = Cloud IAM Complexity Risk Score;
- C = Complexity Component;
- E = Exposure Component;
- $C \times E$ = interaction between complexity and exposure;
- AC = Asset Criticality.

The interaction term is included because the central theoretical assumption of the research is that complexity can amplify existing security exposure.

For example, high permission exposure may be easier to detect and correct in a simple, well-governed environment. The same exposure in an environment containing numerous roles,

indirect relationships, redundant policies, contextual conditions, and weak access-review processes may be substantially more difficult to identify and remediate.

The equation deliberately uses equal contributions for complexity, exposure, and their interaction because there is currently insufficient empirical evidence to justify more precise weighting. Future validation may therefore modify the equation.

4.8 Risk Classification

The resulting score ranges from 0 to 100.

CICRS Score	Risk Level	Interpretation
0-19	Very Low	Limited complexity-related exposure
20-39	Low	Some weaknesses exist but exposure remains relatively controlled
40-59	Moderate	Multiple complexity or exposure factors require remediation
60-79	High	Significant IAM complexity combined with meaningful security exposure
80-100	Critical	Severe privilege, governance, or resource-exposure conditions requiring priority attention

These bands are provisional theoretical classifications and should not be presented as empirically validated thresholds.

4.9 Worked Hypothetical Example

Consider a hypothetical cloud environment with the following normalized dimension scores:

Dimension	Score
Structural Complexity <i>SC</i>	0.70
Policy Quality Weakness <i>PQ</i>	0.60
Permission Exposure <i>PE</i>	0.80
Privilege Propagation <i>PP</i>	0.75
Dynamic Complexity <i>DC</i>	0.40
Governance Weakness <i>GW</i>	0.55
Asset Criticality <i>AC</i>	0.90

Step 1: Calculate Complexity

$$C = \frac{0.70 + 0.60 + 0.40 + 0.55}{4}$$

$$C = 0.5625$$

Step 2: Calculate Exposure

$$E = \frac{0.80 + 0.75}{2}$$

$$E = 0.775$$

Step 3: Calculate Interaction

$$C \times E = 0.5625 \times 0.775$$

$$C \times E = 0.436$$

Step 4: Calculate CICRS

$$CICRS = 100 \times 0.90 \times \frac{0.5625 + 0.775 + 0.436}{3}$$

$$CICRS \approx 53.2$$

The hypothetical environment would therefore be classified as:

Moderate Risk

The score also remains explainable. The relatively high result is driven primarily by **Permission Exposure (0.80)** and **Privilege Propagation (0.75)** rather than by structural complexity alone.

This illustrates an important characteristic of the proposed framework: the final numerical result can be traced back to the dimensions responsible for the risk.

4.10 Model Interpretation

The proposed CICRS should not be interpreted as an absolute prediction that a security incident will occur. Rather, it is intended as a structured method for comparing IAM conditions and identifying environments in which complexity and exposure combine to create greater security concern.

The model provides two levels of interpretation:

Overall assessment: the 0-100 CICRS provides a summarized indication of complexity-related IAM risk.

Diagnostic assessment: the individual dimension scores identify the source of that risk.

For example, two environments could both receive a score of 60 while requiring different remediation strategies. One may have strong governance but severe privilege propagation, while another may have limited escalation paths but extensive policy redundancy and lifecycle weaknesses. Consequently, the individual dimension scores should always accompany the overall score.

4.11 Model Limitations and Validation Requirements

The proposed CICRS is a **theoretical model** derived from the reviewed literature. Its dimensions are literature-grounded, but the normalization thresholds, weighting assumptions, interaction structure, and risk bands have not yet been empirically validated.

Future research should therefore assess the model using:

- Real-world cloud IAM configurations.
- Synthetic misconfiguration scenarios.
- Known privilege-escalation cases.
- IAM practitioner and expert assessment.
- Sensitivity analysis.
- Cross-platform evaluation across AWS, Azure, and Google Cloud.
- Comparison between CICRS scores and independently identified security weaknesses.

Empirical testing would enable the proposed weights and thresholds to be calibrated and determine whether individual indicators should contribute differently to the final risk score.

This qualification is important because your thesis should claim that you have developed a theoretically grounded model, not that you have already proven its predictive accuracy.

Chapter 5 - Discussion and Evaluation

5.1 Discussion of Findings

The findings of this study indicate that cloud IAM complexity is not represented adequately by a single measure such as the number of identities, roles, permissions, or policies. Instead, complexity emerges from the interaction of structural, logical, administrative, contextual, governance, and exposure-related factors.

The literature demonstrates that conventional access-control models provide important mechanisms for structuring authorization but can themselves introduce different forms of complexity. RBAC simplifies direct permission management through roles, but large role structures may create role explosion, overlapping permissions, inheritance complexity, and separation-of-duty conflicts [1], [13]. ABAC provides greater flexibility through attribute-based decisions, but this introduces additional dependencies on policy conditions, attribute sources, environmental context, and attribute accuracy [1], [5], [8].

The review also identified policy quality as an important element of IAM complexity. Complexity, redundancy, maintainability, and authorization accuracy are recognised as relevant IAM measurement areas [3]. Policy quality cannot therefore be assessed purely through policy size. A relatively small policy may still provide excessive access through wildcard actions, broad resource permissions, or indirect authorization relationships.

This is demonstrated particularly clearly by Grasp [6], where relatively small serverless IAM policies could produce extensive connectivity between functions and resources. This supports one of the central arguments of the proposed model: complexity should not be treated as equivalent to risk.

A large IAM configuration can contain many well-defined and appropriately governed relationships while maintaining effective least privilege. Conversely, a smaller configuration may contain a short privilege-escalation path or highly permissive wildcard permission capable of exposing a critical resource.

The findings therefore suggest that IAM complexity should instead be understood as a risk-amplifying condition. Complexity becomes security-relevant when it reduces visibility, weakens governance, increases the difficulty of identifying excessive privileges, or creates indirect paths to sensitive resources.

Privilege propagation is particularly important in this respect. Existing privileges do not necessarily represent the maximum authority that an identity can obtain. TAC [7] demonstrates that permissions may propagate through relationships among users, groups, roles, services, and permissions. Consequently, effective risk assessment should consider both current permissions and potential future permissions that can be obtained through allowed IAM actions.

Graph-based approaches reinforce this finding. Reachability analysis [6] can identify whether identities or services can reach resources indirectly, while attack-graph research [12], [14] demonstrates how paths and dependencies can represent security exposure. These approaches influenced the Privilege Propagation and Permission Exposure dimensions of the proposed model.

Governance was also identified as a significant component. Lifecycle failures, dormant accounts, delayed revocation, ineffective access reviews, and separation-of-duty weaknesses can cause inappropriate access to remain active even when the underlying technical mechanisms function correctly [2]-[4]. The inclusion of Governance Weakness therefore ensures that the proposed model does not assess IAM purely as a technical policy problem.

Overall, the findings support a multidimensional approach in which complexity, exposure, propagation, governance, contextual conditions, and asset importance are assessed together.

5.2 Evaluation of the Proposed Model

The Cloud IAM Complexity Risk Score (CICRS) was developed as a theoretical and explainable model rather than as a predictive security system. Its evaluation therefore focuses on conceptual properties rather than measures such as predictive accuracy or incident-detection performance.

5.2.1 Literature Coverage

The model provides broad coverage of the main factors identified across the reviewed studies. Structural complexity is informed by access-control structures and RBAC relationships [1], [13]. Policy Quality and Maintainability Weakness draws particularly from IAM metrics and policy-quality research [3], [9]. Permission Exposure and Privilege Propagation incorporate excessive authorization, reachability, and privilege-escalation concepts [3], [6], [7]. Dynamic and Contextual Complexity reflects findings relating to context-aware, fog, and distributed access control [8], [10], [11]. Governance Weakness incorporates lifecycle, access-review, and enterprise IAM requirements [2]-[4].

The seven dimensions therefore provide reasonable conceptual coverage of the factors identified within the selected literature.

5.2.2 Logical Coherence

A principal strength of the model is the separation between complexity and security exposure.

The Complexity Component combines:

$$SC, PQ, DC, GW$$

while the Exposure Component combines:

$$PE, PP$$

Asset Criticality is subsequently used to represent potential impact.

This structure avoids the assumption that an environment becomes insecure simply because it becomes large or complicated. The interaction term between complexity and exposure reflects

the theoretical proposition that complexity can amplify security risk when meaningful exposure already exists.

5.2.3 Traceability

Each component of CICRS can be traced to an underlying dimension and subsequently to individual indicators. For example, a high overall score caused by Permission Exposure can be examined further through excessive permissions, sensitive-resource reachability, privileged access, or wildcard permissions.

This improves transparency compared with a single aggregated score whose origin cannot be explained.

Traceability is particularly important because the purpose of the proposed model is not simply to classify an environment but also to indicate why a particular risk assessment was produced.

5.2.4 Explainability

Explainability is supported using clearly defined dimensions, normalized indicators, explicit mathematical aggregation, and separate reporting of individual dimension scores.

The overall CICRS should therefore be presented together with the dimension-level results. This allows an administrator to distinguish, for example, between an environment whose score is primarily caused by weak governance and one whose score is driven by privilege-escalation paths.

This is preferable to treating the overall numerical value as an independent security conclusion.

5.2.5 Measurability

Most of the proposed indicators could theoretically be derived from cloud IAM configuration information. Examples include numbers of roles, policies and trust relationships, wildcard permissions, privilege paths, dormant accounts, access-review status, and resource sensitivity.

However, some indicators are more difficult to measure objectively. Policy understandability, business criticality, and governance quality may require organisational knowledge or expert judgement. Consequently, future implementation would require precise measurement definitions for each indicator.

5.2.6 Distinctiveness

The comparative analysis demonstrates that existing studies tend to focus on specific parts of the IAM problem. IAM metric research identifies relevant measurements [3]; formal verification examines policy correctness [5]; Grasp analyses reachability [6]; TAC examines privilege escalation [7]; and attack-graph research models security paths and dependencies [12], [14].

The contribution of CICRS is therefore not to replace these approaches, but to integrate concepts derived from them into a broader cloud IAM complexity-risk framework.

5.2.7 Sensitivity

Because all dimensions are normalized between 0 and 1, changes in individual values influence the final score in a transparent way. Higher Permission Exposure or Privilege Propagation increases the Exposure Component, while increases in Structural Complexity, Policy Quality Weakness, Dynamic Complexity, or Governance Weakness increase the Complexity Component.

The interaction term causes risk to increase further when both complexity and exposure are high. However, the current study does not provide empirical sensitivity testing across a real dataset. Consequently, sensitivity analysis remains a requirement for future validation.

5.3 Answers to the Research Questions

RQ1: What factors contribute to complexity within cloud IAM environments?

The study identifies several related contributors to cloud IAM complexity. These include the number and relationships of identities, roles, permissions, policies, resources, trust relationships, policy conditions, contextual attributes, distributed authorization domains, governance processes, and privilege relationships.

These factors were consolidated into Structural Complexity, Policy Quality and Maintainability Weakness, Dynamic and Contextual Complexity, Governance Weakness, Permission Exposure, Privilege Propagation, and Asset Criticality.

RQ2: How does cloud IAM complexity contribute to security risk?

The findings suggest that complexity is not itself a vulnerability. Rather, increasing complexity may reduce visibility and make authorization relationships more difficult to understand, review, maintain, and revoke.

This can increase the likelihood that excessive permissions, incorrect policies, dormant access, unintended resource reachability, or privilege-escalation paths remain unidentified. Complexity therefore operates primarily as a risk amplifier when combined with actual security exposure and governance weaknesses.

RQ3: Which measurable IAM dimensions and indicators are suitable for inclusion in a theoretical model?

The study identifies seven principal dimensions:

1. Structural Complexity;
2. Policy Quality and Maintainability Weakness;
3. Permission Exposure;
4. Privilege Propagation;
5. Dynamic and Contextual Complexity;

6. Governance Weakness; and
7. Asset Criticality.

Potential indicators include role hierarchy depth, policy redundancy, wildcard permissions, excessive authorization, sensitive-resource reachability, privilege-escalation paths, dormant identities, overdue access reviews, contextual attributes, trust relationships, and resource sensitivity.

RQ4: How can the selected indicators be organised into an explainable theoretical risk-scoring model?

The proposed CICRS normalizes indicators to a common 0-1 scale and aggregates them into dimensions. Structural Complexity, Policy Quality, Dynamic Complexity, and Governance Weakness form the Complexity Component, while Permission Exposure and Privilege Propagation form the Exposure Component.

The model then combines complexity, exposure, their interaction, and Asset Criticality to generate a score between 0 and 100.

The model remains explainable because the overall score can be decomposed back into its contributing dimensions and indicators.

RQ5: How can the proposed theoretical model be evaluated?

At the current stage, the model can be evaluated according to literature coverage, conceptual coherence, traceability, explainability, measurability, distinctiveness, and potential applicability.

Predictive accuracy cannot currently be assessed because the model has not been tested against operational IAM datasets. Empirical validation is therefore required before the model can be considered suitable for practical risk prediction.

5.4 Comparison with Existing Approaches

The proposed model differs from existing work primarily through integration.

Access-control surveys [1], [8]-[11], [13] explain how authorization can be structured and identify challenges associated with increasingly dynamic and distributed environments. However, these approaches do not provide an integrated cloud IAM complexity-risk score.

IAM measurement research [3] identifies metrics relating to authorization accuracy, complexity, redundancy, maintainability, security, and process quality. CICRS builds upon these concepts by selecting risk-relevant indicators and positioning them within a wider assessment framework.

Formal verification [5] provides methods for identifying logical policy problems but cannot independently establish whether formally valid policies create excessive business risk.

Grasp [6] and TAC [7] provide more security-oriented analysis through reachability and privilege propagation. These approaches strongly influence the Permission Exposure and Privilege Propagation dimensions, but their primary purpose is not to measure the overall complexity-related risk of an IAM environment.

Network attack-graph approaches [12], [14] further demonstrate the usefulness of modelling dependencies and attack paths. CICRS adapts this reasoning to IAM while combining it with policy, governance, contextual, and asset-related factors.

The proposed model can therefore be understood as a synthesis framework that connects concepts that existing studies normally analyse separately.

5.5 Limitations of the Study

First, the research is based on a relatively small, selected corpus. Although the studies cover several important aspects of IAM and access control, the literature set cannot represent every cloud IAM technology, implementation, or security problem.

Second, some of the reviewed security research is particularly focused on AWS [5]-[7]. Although many underlying concepts such as privilege propagation and reachability can be generalised, cloud providers implement IAM differently. The model therefore requires evaluation against Azure, Google Cloud, and multi-cloud environments.

Third, the model has not been empirically validated. The normalization thresholds, equal weighting approach, interaction term, asset-criticality values, and risk classification bands remain theoretical.

Fourth, some indicators may require organisational judgement. For example, resource criticality and policy maintainability cannot always be determined directly from technical configuration data.

Finally, the overall risk score simplifies a complex security environment into a numerical value. The score should therefore supplement rather than replace detailed security analysis. Dimension-level results remain necessary for meaningful interpretation.

5.6 Practical and Research Implications

If empirically validated, CICRS could provide cloud-security teams with a structured method for examining IAM environments beyond simple policy counts or isolated configuration findings.

The model could potentially support identification of environments where high structural complexity coincides with excessive permissions, privilege propagation, weak governance, or sensitive-resource exposure. The dimension-level structure could also support prioritisation by showing which aspects contribute most strongly to the overall assessment.

From a research perspective, the model provides a foundation for investigating whether measurable IAM complexity is statistically associated with security exposure,

misconfiguration, privilege escalation, or security incidents. However, practical use should remain conditional on future calibration and empirical validation.

Chapter 6 - Conclusion and Future Work

6.1 Conclusion

Cloud IAM has developed into a highly interconnected security environment involving human and non-human identities, roles, permissions, policies, attributes, trust relationships, distributed resources, and governance processes. Existing research demonstrates that these elements can create significant administrative and security challenges, particularly when authorization relationships become difficult to understand or maintain.

This study addressed the identified gap by developing a Theoretical Cloud IAM Complexity Risk-Scoring Model (CICRS). The central finding is that IAM complexity should not automatically be interpreted as security risk. Complexity becomes more security-relevant when it interacts with factors such as excessive permissions, privilege propagation, weak policy quality, ineffective governance, and exposure of important resources.

The proposed model therefore separates complexity from direct exposure and impact. Seven dimensions were identified: Structural Complexity, Policy Quality and Maintainability Weakness, Permission Exposure, Privilege Propagation, Dynamic and Contextual Complexity, Governance Weakness, and Asset Criticality. These dimensions are normalized and combined into Complexity and Exposure components before being incorporated into an explainable overall risk score.

The proposed framework provides a structured theoretical basis for understanding not only how complex an IAM environment is, but also whether that complexity is associated with meaningful security exposure.

6.2 Achievement of Aim and Objectives

The research aim was to develop a theoretical risk-scoring model for assessing security risks associated with cloud IAM complexity.

This aim was addressed through the four research objectives.

Review: Existing literature relating to IAM, access-control models, policy quality, IAM metrics, privilege escalation, distributed authorization, formal verification, reachability, and attack graphs was reviewed to identify relevant concepts and existing approaches.

Analyse: The findings were analysed to identify relationships between IAM complexity and security risk. This analysis demonstrated the importance of distinguishing complexity from actual exposure.

Build: The identified factors were consolidated into seven measurable dimensions and incorporated into the proposed CICRS framework, including normalization, aggregation, complexity-exposure interaction, asset criticality, and provisional risk classifications.

Evaluate: The model was evaluated theoretically according to coverage, coherence, traceability, explainability, measurability, distinctiveness, applicability, assumptions, and limitations.

The four objectives have therefore been addressed at a theoretical level.

6.3 Research Contribution

The primary contribution of this research is an integrated and explainable theoretical framework for assessing cloud IAM complexity-related security risk. Existing research provides valuable mechanisms for evaluating individual concerns such as IAM metrics [3], policy verification [5], reachability [6], privilege escalation [7], and attack paths [12], [14]. However, these areas are generally addressed independently. CICRS brings these concepts together within a single model.

A second contribution is the explicit distinction between complexity and risk. The model does not assume that a larger or more interconnected environment is automatically less secure. Instead, risk emerges from the interaction between complexity, exposure, governance, privilege relationships, and asset importance.

A third contribution is explainability. Rather than producing only an overall numerical score, the framework retains separate dimensions that allow the reasons behind the assessment to be examined.

The contribution should nevertheless be considered theoretical until empirical testing establishes whether the proposed indicators, weights, thresholds, and aggregation mechanism correspond reliably with real cloud-security conditions.

6.4 Future Work

The most important future activity is empirical validation of the proposed model. Future research should test CICRS against real-world or representative IAM configurations containing known security conditions. This could include intentionally misconfigured cloud environments, publicly available IAM datasets, synthetic configurations, or anonymised organisational data.

The proposed normalization thresholds also require calibration. Rather than relying on theoretically selected values, future studies could establish baseline distributions for indicators such as role hierarchy depth, wildcard permission frequency, access-review delay, privilege-path length, and trust-relationship density.

The current equal-weighting approach should also be evaluated. Alternative weights could be established using expert elicitation, Analytic Hierarchy Process, statistical modelling, historical incident analysis, or other empirical techniques.

Cross-cloud validation is another important requirement. The current evidence base contains significant AWS-oriented research. Future work should therefore determine whether the dimensions and metrics remain appropriate for Microsoft Azure, Google Cloud Platform, and hybrid or multi-cloud environments.

Future research could also examine automated graph generation from cloud IAM configurations. Identities, roles, policies, resources, permissions, and trust relationships could potentially be represented as graph structures from which reachability, privilege propagation, centrality, path length, and related indicators could be calculated automatically.

Finally, longitudinal evaluation could investigate whether changes in CICRS are associated with improvements or deterioration in IAM security over time. Such research would help determine whether the score can function not only as a theoretical assessment mechanism but also as a practical security-management metric.

Until these validation activities are completed, CICRS should be interpreted as a literature-grounded theoretical framework rather than a validated predictor of cloud-security incidents.

References

- [1] R. El Sibai, N. Gemayel, J. Bou Abdo, and J. Demerjian, “A survey on access control mechanisms for cloud computing,” *Trans. Emerging Telecommun. Technol.*, vol. 31, Art. no. e3720, 2020, doi: 10.1002/ett.3720.
- [2] I. Indu, P. M. Rubesh Anand, and V. Bhaskar, “Identity and access management in cloud environment: Mechanisms and challenges,” *Eng. Sci. Technol., Int. J.*, vol. 21, pp. 574-588, 2018, doi: 10.1016/j.jestch.2018.05.010.
- [3] T. Baumer, S. Kern, L. Fuchs, and G. Pernul, “Identity and access management metrics: A systematic review,” *ACM Comput. Surv.*, vol. 58, no. 8, Art. no. 213, Feb. 2026, doi: 10.1145/3788858.
- [4] J. Glöckler, J. Sedlmeir, M. Frank, and G. Fridgen, “A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity,” *Bus. Inf. Syst. Eng.*, vol. 66, no. 4, pp. 421-440, 2024, doi: 10.1007/s12599-023-00830-x.
- [5] E. Zahoor, Z. Asma, and O. Perrin, “A formal approach for the verification of AWS IAM access control policies,” in *Proc. 6th Eur. Conf. Service-Oriented and Cloud Computing (ESOCC)*, Oslo, Norway, 2017, pp. 59-74, doi: 10.1007/978-3-319-67262-5_5.
- [6] I. Polinsky, P. Datta, A. Bates, and W. Enck, “Grasp: Hardening serverless applications through graph reachability analysis of security policies,” in *Proc. ACM Web Conf. 2024 (WWW '24)*, Singapore, 2024, pp. 1643-1654, doi: 10.1145/3589334.3645436.
- [7] Y. Hu and W. Wang, “TAC: Hybrid IAM privilege escalation detection,” unpublished manuscript.
- [8] A. S. M. Kayes, R. Kalaria, I. H. Sarker, M. S. Islam, P. A. Watters, A. Ng, M. Hammoudeh, S. Badsha, and I. Kumara, “A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues,” *Sensors*, vol. 20, no. 9, Art. no. 2464, Apr. 2020, doi: 10.3390/s20092464.

- [9] L. Golightly, P. Modesti, R. Garcia, and V. Chang, “Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN,” *Cyber Security Appl.*, vol. 1, Art. no. 100015, 2023, doi: 10.1016/j.csa.2023.100015.
- [10] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, “Access control for emerging distributed systems,” *Computer*, vol. 51, no. 10, pp. 100-103, Oct. 2018.
- [11] P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au, and X. Luo, “A survey on access control in fog computing,” *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 144-149, Feb. 2018, doi: 10.1109/MCOM.2018.1700333.
- [12] C. Phillips and L. P. Swiler, “A graph-based system for network-vulnerability analysis,” in *Proc. New Security Paradigms Workshop (NSPW '98)*, Charlottesville, VA, USA, 1998, pp. 71-79.
- [13] R. Sandhu, D. Ferraiolo, and R. Kuhn, “The NIST model for role-based access control: Towards a unified standard,” in *Proc. 5th ACM Workshop Role-Based Access Control (RBAC 2000)*, Berlin, Germany, 2000, pp. 47-63.
- [14] X. Ou, W. F. Boyer, and M. A. McQueen, “A scalable approach to attack graph generation,” in *Proc. 13th ACM Conf. Computer and Communications Security (CCS '06)*, Alexandria, VA, USA, 2006, pp. 336-345.