

Cloud-Based Identity and Access Management for Strengthening Enterprise Cyber Resilience in Saudi Arabia

Yahya Khalil

0009-0004-0870-3795

Published October 2026

Abstract

Saudi companies are transferring their applications, data, collaboration platforms, and key business processes into public, private, and hybrid cloud environments. While this shift enhances scalability and service agility, it also undermines the assumption that users, devices, and workloads can be trusted since they come from an internal network. As a result, identity and access management now serves as a means of achieving cyber resilience rather than remaining just an administrative task. This report brings together research that was published between 2020 and 2025 on cloud identity management, multi-factor authentication, federated identity, attribute-based authorization, zero-trust access, identity-as-a-service, continuous monitoring, and resilient cloud security. Its objective is to examine how identity-focused controls can help reduce unauthorized access, restrict lateral movement, ensure service continuity, and speed up recovery in Saudi enterprise settings that are in line with Vision 2030. In order to achieve this, a structured integrative review was carried out, selecting thirty publications verified by DOI and directly relevant to the subject, with clear methodological standards and practical applicability to distributed enterprise systems. The synthesis indicates that resilient IAM relies on six interdependent capabilities: authoritative management of the identity lifecycle, phishing-resistant authentication, context-aware authorization, disciplined handling of privileged access, continuous telemetry, and automated revocation and recovery. Protection provided by isolated controls is very limited if problems such as entitlement drift, weaknesses in federation, compromised end points, or out-of-date credentials are not dealt with. The paper puts forward an identity-centric cloud cyber-resilience framework which connects preventive access decisions with detection, response, recovery, and governance. For Saudi enterprises, the main consequence is that cloud IAM should be treated as a continuously assured control plane that links security architecture, regulatory compliance, workforce practices, and operational resilience rather than being viewed merely as a login service.

1 Introduction

The move to cloud computing alters the location of systems and, more significantly, changes the foundation upon which trust is built. Nowadays, enterprise users access software-as-a-service platforms, cloud infrastructure, application programming interfaces, and distributed data repositories from their offices, their homes, mobile devices, partner networks, and automated workloads. As a result, the traditional security boundary becomes fragile. Studies into cloud security consistently point to access issues, account hijacking, weak credentials, insider misuse, privacy breaches, and configuration errors as ongoing risks [1,2]. Because of this, identity and access management (IAM) has moved from being merely a function for managing an administrative directory to becoming a security control plane. Contemporary IAM includes identity verification, account provisioning, authentication, federation, authorization, privilege governance, session management, logging, access

reviews, and deprovisioning. Cloud IAM also has to deal with non-human identities such as services, applications, containers, automation accounts, and application programming interfaces. A failure at any stage of that lifecycle can provide a route to compromise even if the networks and end points are otherwise well protected. Therefore, reviews of cloud identity management stress that authentication and authorization must be treated as closely linked mechanisms, with policies able to function across different providers and organizational boundaries [3,4].

Cyber resilience offers a broader viewpoint than preventive cybersecurity; an enterprise that is resilient needs to anticipate adverse events, be able to withstand disruption, limit the extent of the impact, restore essential services, and adjust its controls following an incident. Although cloud architectures can enhance resilience by means of redundancy and rapid provisioning, the same connectivity may also increase the risk of credential theft, privilege escalation, and lateral movement. Research into intelligent cloud systems therefore connects security with resilience and claims that protection should include the various layers, services, and interactions which enable a cloud system to keep on operating and to recover from an attack [5]. Identity plays a key role in this relationship since most legitimate and malicious actions are carried out through an identity, a credential, a token, or a workload principal.

The research into zero trust supports this idea that the focus should be on identity. Instead of considering an internal network to be inherently reliable, zero trust demands that each access decision be explicitly verified and that authorization be strictly limited. Research on designs that are intended to be resilient indicates that resilience is enhanced when access control stays dependable even if a component is compromised and when recovery is built into the architecture rather than being introduced after a failure [6]. Further reviews have identified identity, authentication, authorization, device condition, contextual risk, and continuous assessment as key aspects of implementing zero trust [7-11]. Nevertheless, the literature also cautions that zero trust is not a single product and that badly designed implementations can lead to increased cost, higher latency, greater policy complexity, and more user friction [8,12].

This is particularly important in Saudi Arabia, where Vision 2030 has sped up digital government, increased the use of the cloud, modernised platforms, and promoted data-driven services. Research carried out in Saudi Arabia shows that cybersecurity practices have a positive relationship with the quality and trustworthiness of digital services, and that security outcomes are influenced by investment, training, infrastructure, and compliance with regulations [2,30]. Further studies into the adoption of secure community-cloud solutions in the country indicate that organisational acceptance relies on awareness, perceived security, and institutional readiness [29]. The problem is therefore not merely one of implementing more robust authentication; Saudi businesses need an identity and access management (IAM) model which enables rapid digital growth while at the same time maintaining the principles of least privilege, evidence retention, continuity, and recoverability within their hybrid and multi-cloud environments.

The review meets this need by looking at the way cloud-based identity and access management can enhance enterprise cyber resilience in Saudi Arabia. Rather than viewing IAM as a separate technology area, it examines how aspects such as identity lifecycle governance, the strength of authentication, the level of authorization, federation, privileged access, telemetry, and automated response relate to the resilience goals of resistance, containment, recovery, and learning. This framework is meant to assist with architecture decisions, governance design, and future empirical research within Saudi enterprises.

2 Aim, objectives and review questions

This study seeks to combine the latest evidence regarding cloud-based identity and access management and to examine how identity-focused security measures can enhance the cyber resilience of enterprises in Saudi Arabia. The review is guided by four objectives. The first of these is to look at the ways in which cloud identity threats emerge from the use of distributed users, workloads, credentials, federation relationships, and multi-cloud administration. The second objective is to assess the authentication and authorization mechanisms that are capable of reducing unauthorized access and the occurrence of excessive privileges. The third involves linking identity and access management controls to resilience outcomes such as containment, continuity, incident response, and recovery. The fourth objective is to create a governance framework that is suited to the digital transformation of enterprises in Saudi Arabia within the context of Vision 2030.

The article looks at four questions: the first of these investigates which cloud IAM features are most consistently linked with greater security and resilience. The second question examines how zero-trust, multifactor authentication, federation, and attribute-based access control affect the enterprise access model. The third question looks into which implementation flaws can weaken even well-established IAM programs. The fourth question is about how Saudi enterprises can set up identity governance so that security, regulatory assurance, and operational continuity support one another rather than clash. These questions intentionally focus on the relationships between different controls rather than assessing a particular vendor platform.

3 Review methodology

An integrative review based on a structured approach was chosen since the subject area includes technical security mechanisms, enterprise architecture, governance, and research into Saudi digital transformation. The method was intended to maintain the transparency characteristic of a systematic review while at the same time preventing the need for artificial screening figures. The literature was identified using scholarly searches and publisher databases that cover research on computer security, cloud computing, information systems, and digital government. The search terms included those relating to identity and access management, cloud identity, multifactor authentication, federation, identity-as-a-service, attribute-based access control, zero trust, least privilege, cyber resilience, cloud security, Saudi Arabia, and Vision 2030.

The time frame for the publication was limited to the period 2020 to 2025; earlier foundational concepts were mentioned only when required to understand the more recent work and were not part of the thirty-reference analytical corpus. Only peer-reviewed journal articles or comprehensive research reviews with a resolvable DOI, which were clearly relevant to cloud IAM or enterprise resilience and contained sufficient methodological or architectural detail to allow for synthesis, were considered eligible. Those sources that concentrated solely on unrelated cryptographic primitives, on consumer authentication lacking enterprise implications, or on access scenarios that were not cloud-based were excluded. Where evidence specific to Saudi Arabia addressed cloud adoption, digital transformation, cybersecurity capability, or e-government security, it was included, even if IAM was not the only dependent variable, since such studies provide the background on the national implementation context [2,29,30].

The corpus that was ultimately produced consisted of thirty publications. The DOI entries were verified by referring to the publishers' or bibliographic pages, and all the citations were limited to the period between 2020 and 2025. When assessing the quality five different aspects were taken into

account: the clarity of purpose, the transparency of the methods, the technical specificity, the extent to which the claims were supported by evidence, and the relevance to actual enterprise deployment. Review and survey papers were employed in order to identify concepts and the challenges that occurred repeatedly, whereas experimental and architectural studies were used to determine whether the proposed mechanisms dealt with specific problems such as compromised credentials, excessive privilege, policy expressiveness, privacy, or lateral movement. A numerical quality score was not applied since the varied study designs could make a single score misleading.

The data extraction process used an analytical matrix consisting of seven fields: the identity object, the threat or failure mode, the control mechanism, the authorization model, the monitoring requirement, the resilience contribution, and the implementation constraint. This approach allowed studies that employed different terminology to be compared. For instance, a paper on zero trust might talk about continuous trust evaluation, while one on identity and access management might refer to adaptive or risk-based authorization; in both cases, these were categorized under contextual decision making since the access decision changed in response to the observed conditions. Likewise, revocation, session termination, credential rotation, and rapid deprovisioning were all classified as recovery actions because they reduced the attacker's continued access.

The process took place in three stages. In the first stage, the findings were divided into the themes of identity lifecycle, authentication, authorization, federation, monitoring, and recovery. In the second stage, the relationships between these themes were looked at in order to determine the control dependencies. In the third stage, the themes were assigned to the resilience functions: anticipate, withstand, contain, recover, and adapt. This assignment showed an important difference: controls like multifactor authentication mainly reduce the probability of unauthorized access, while continuous authorization and rapid revocation reduce the length of time and the extent of the impact of a compromise once access has occurred. Cyber resilience thus relies on the combination of these measures rather than on any one of them.

The method has two intentional limits: it does not assert that the thirty papers cover every publication on cloud IAM, and it does not draw Saudi-specific causal conclusions from studies carried out in other places. Rather, the global technical evidence is combined with research focusing on Saudi organizations and policies. This way of proceeding is appropriate for developing a defensible conceptual framework and at the same time makes it clear that further longitudinal and sector-specific verification within the local context is still needed.

Table 1. Review scope and analytical dimensions.

Dimension	Review focus	Resilience interpretation
Identity lifecycle	Provisioning, changes, deprovisioning, ownership	Reduces stale accounts and restores trusted identity state
Authentication	MFA, phishing resistance, device and contextual signals	Lowers probability of unauthorized entry and enables step-up assurance
Authorization	RBAC, ABAC, least privilege, just-in-time access	Constrains blast radius and privilege escalation
Federation and IDaaS	SSO, trust relationships, token and provider dependency	Extends control across clouds while managing concentration risk
Observability	Sign-in, session, privilege and behavior telemetry	Supports early detection and risk-adaptive decisions

Dimension	Review focus	Resilience interpretation
Response and recovery	Revocation, session termination, credential rotation	Shortens attacker dwell time and rebuilds trusted access
Saudi enterprise context	Cloud adoption, governance, digital services, workforce readiness	Aligns IAM with Vision 2030 continuity and assurance goals

4 Cloud IAM as a resilience control plane

Identity management must start before the process of authentication takes place. In order to do this, an organisation needs reliable sources for its employees, contractors, partners, customers, devices, and workloads, along with the proper procedures for creating, updating, suspending, and removing access rights. Since cloud environments make errors in the lifecycle of accounts more dangerous, a dormant account or service credential can stay accessible from the internet and may continue to have permissions on a number of different platforms. For these reasons, the relevant literature regards identity governance as an ongoing management issue and not as a single event such as the initial creation of an account [3,4]. A robust design should link the identity lifecycle to human-resource events, the end dates of contractor agreements, application ownership, asset inventories, and the cloud provisioning processes.

Authentication allows one to be certain that a subject is indeed the one or thing it says it is. Password-based systems are becoming more and more unsuitable since attacks such as phishing, credential stuffing, token theft, and social engineering are able to overcome fixed secrets. Studies that focus on the cloud suggest the use of multifactor and multilayer authentication, which combines evidence relating to possession, knowledge, the device, biometrics, or behaviour [4,13,14]. The benefit of more robust authentication is not just that there will be fewer breaches; it also provides incident responders with more reliable evidence so that they can tell the difference between a compromised session and normal activity and allows for step-up verification when the level of risk changes. Yet the MFA system has to be designed to guard against fatigue attacks, insecure recovery methods, and token replay; otherwise, adding more factors without protecting the entire authentication process can result in only a superficial level of assurance.

The things that an authenticated user is allowed to do are determined by authorization. While role-based access control is still useful in practice, cloud environments usually demand more detailed decisions taking into account the department, the sensitivity of the resource, the device's security status, the user's location, the type of transaction, the time of the action, and the level of risk. Attribute-based access control is able to express such conditions and can support hierarchical or semantic policies when dealing with distributed resources [15-17]. Research into secure cloud file sharing and cryptographic access control demonstrates that fine-grained policies can also be used to protect data when the infrastructure is shared or only partly trusted [18-20]. The problem in practice is policy governance: unless attributes have authoritative ownership and clear meanings, highly expressive rules can become inconsistent, difficult to test, and hard to explain.

Federation and the provision of identity as a service extend identity and access management beyond both organizational and technical limits. While federated identity eliminates the need for repeated credentials and makes it easier to gain access to various cloud services, a breach of an identity provider can have widespread effects. As a result, research into cloud-based identity federation and IDaaS places particular emphasis on trust relationships, privacy, organizational dependence, and the implications of centralizing authentication [21,22]. The aim with regard to resilience is not to elimin-

ate federation but rather to design it in such a way that trust can be contained, kept under observation, and cancelled if necessary. To achieve this it is necessary to carry out the rotation of certificates and keys, use tokens that are restricted to specific audiences, apply short session durations where appropriate, establish clear fallback procedures, and have tested protocols in place for the event of an identity provider failure.

Zero Trust incorporates these capabilities into a continuous access model; it changes the security issue from one of whether or not a user has crossed a network boundary to one of whether a particular identity, device, workload, and request should be given a specific privilege at this moment. Surveys have consistently found authentication, authorization, micro-segmentation, trust assessment, and policy enforcement to be interdependent elements [9-12]. A robust IAM program is thus the practical basis of zero trust, although zero trust also alters IAM by requiring that evaluations be carried out after each login. Instead of being a single event, the access decision becomes a process.

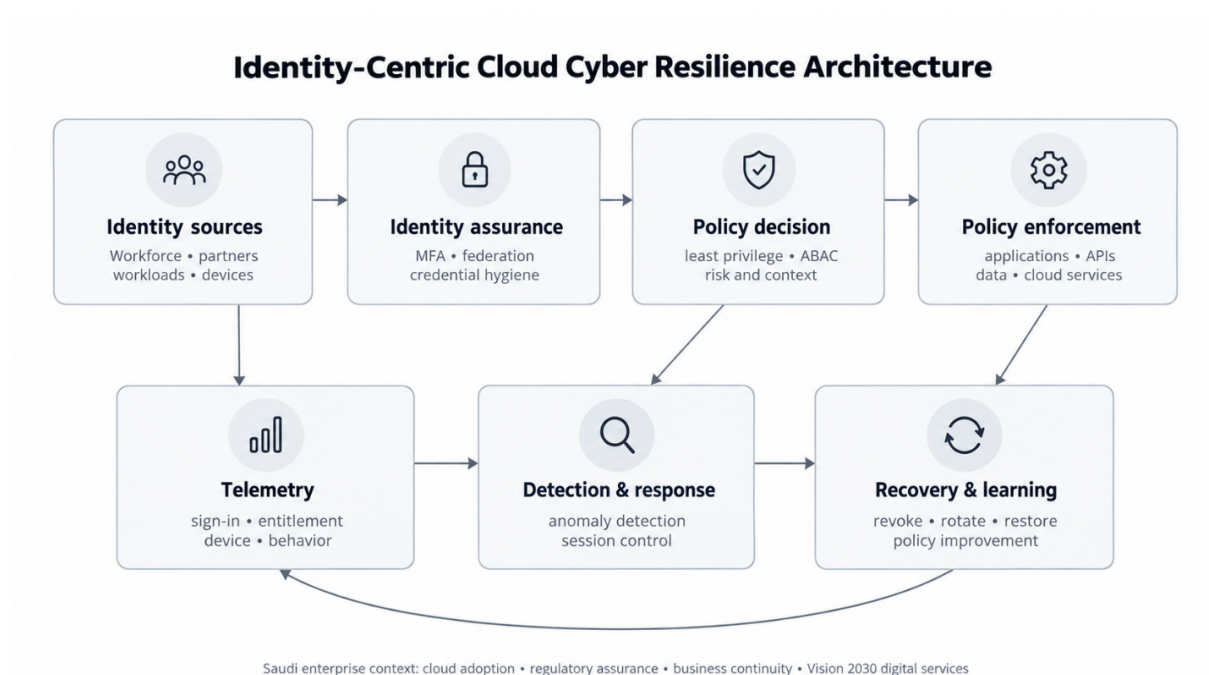


Figure 1. Identity-centric cloud cyber resilience architecture for Saudi enterprise environments.

5 Mechanisms linking IAM to cyber resilience

The initial way to build resilience is to reduce the extent of the compromise. This can be achieved through strong identity verification, the use of phishing-resistant multi-factor authentication, controlled enrolment, protection of credentials, and access that is aware of the device, all of which lower the chance that stolen passwords will lead to immediate access. The multifactor systems designed for cloud applications show how authentication can be combined with access policies and intrusion detection rather than being used as a stand-alone gateway [13]. Reviews of cloud authentication also indicate that no single factor is adequate for all possible threat situations [4,14]. For businesses, the practical result is to base the level of authentication on the importance of the resource and the risk associated with the user, rather than applying the same level of control to all transactions.

The second method involves limiting the blast radius. By applying the principle of least privilege, it is possible to restrict the extent to which a compromised identity can access resources. As zero-trust research has shown, continuously validated, access that is specific to resources is more resilient than allowing broad network access since attackers cannot automatically use one set of credentials to gain unrestricted movement within the network [6-12]. Attribute-based models increase precision by taking into account the subject, the object, the action, and the environment, while hierarchical systems help to reduce the duplication of policy structures in complex cloud datasets [15,16]. When it comes to resilience, the important figure is not just the percentage of users who have been given multi-factor authentication; it is the amount of privilege that becomes exposed if one identity, role, or token is compromised.

The third mechanism is known as privilege freshness. Enterprise access is constantly changing since employees change roles, projects come to an end, suppliers replace their personnel, and applications are withdrawn. Privileges build up more quickly than they are taken away when authorization is static. This results in an increase in the number of hidden ways that an attacker can carry out an attack. Cloud IAM should therefore provide automation for the joiner-mover-leaver process, time-limited access, regular access certification, checks to ensure separation of duties, and just-in-time privileged elevation. These controls turn privilege from something that is held permanently into a temporary ability. They also enhance recovery since an incident team can remove or restrict access without having to rebuild the whole network segment.

The fourth mechanism is continuous observability. Identity telemetry covers authentication failures, successful logins, token issuance, impossible travel, device posture, changes in privilege, administrative actions, API usage, and anomalous access to resources. Studies into zero-trust and risk-aware access control have demonstrated that contextual signals can be used in dynamic decisions rather than being employed solely for use after an incident has occurred [10,11,23]. The aim is not to automatically deny all unusual events. In a well-developed design, different signals are distinguished according to whether they lead to logging, step-up authentication, reduction of privileges, termination of the session, or the need for a human to intervene. This stepwise response minimises disruption while at the same time enabling the security position to become more stringent as further evidence is gathered.

The fifth mechanism is resilient federation. Although single sign-on enhances usability and can strengthen control by centralising policy, it also introduces concentration risks. If the identity provider, the signing key, the federation metadata, or the administrative plane is compromised, many of the relying applications may accept malicious assertions. Resilience therefore demands redundant identity services, protected signing material, controlled trust configurations, the ability to carry out emergency revocation, and regular testing of the various failure modes. Research into federated and cloud identity systems shows that trust relationships must be explicitly modelled and that outsourcing identity and access management can give rise to privacy and dependency issues [21,22]. A resilience assessment should inquire into what occurs when the identity provider is unavailable, not just how well it functions when it is operating normally.

The sixth aspect relates to non-human identities. In today's cloud environments, the number of service accounts, application identities, containers, managed identities, API keys, certificates and automation tokens usually exceeds that of human users. These identities can be given wide-ranging privileges and are not subject to the kind of multi-factor authentication that applies to people. Nevertheless, the same IAM principles remain valid: authoritative ownership, the use of short-lived

credentials, workload attestation, the principle of least privilege, secret rotation and observable usage. Nowadays, zero-trust models for cloud-native systems place greater emphasis on service identity since microservices communicate across different locations and clouds without benefiting from a fixed network perimeter [9,24]. Failure to address workload identity results in a significant gap between a well-governed workforce IAM programme and the real ways in which cloud data is accessed.

The seventh mechanism involves designing identity in a way that respects privacy. When identity and access management is centralised, it collects a number of sensitive details, including login histories, data from devices, and behavioural indicators. While this enhances security, it also gives rise to privacy and concentration risks. Studies into self-sovereign identity and privacy-preserving access control look at how verifiable credentials, decentralised identity, and selective disclosure can reduce the unnecessary exposure of identity attributes [20,25]. Although these approaches have not yet completely replaced enterprise IAM everywhere, they do show an important point namely that authorization usually requires proof that a condition has been met, not the unrestricted disclosure of all the underlying identity data. Enterprises in Saudi Arabia that are dealing with regulated personal or sectoral data should include data minimisation in the telemetry and federation design of their IAM systems.

The eighth mechanism is response automation; once identity risk has been confirmed, resilience requires speed. Manual tickets might be too slow to deal with token theft or a compromise of privileged accounts. Automated workflows are capable of revoking sessions, disabling accounts, rotating credentials, removing role assignments, isolating devices, or requiring reauthentication. Yet automation must have safeguards since incorrect revocation could itself disrupt essential services. The superior approach is policy-driven automation incorporating severity thresholds, break-glass accounts, approval procedures for significant actions, and immutable evidence of the changes made. In this way, IAM becomes an active incident-response system rather than a passive directory.

In the end, recovery involves restoring the trusted identity state. If credentials, tokens, or privileges have been compromised, it is not enough simply to get the applications back online after an attack; recovery must include resetting the credentials, rotating the keys and certificates, revalidating the privileged accounts, reviewing the federation trust, reconstructing the critical entitlements, and making sure that emergency access has been closed. As the literature on cloud resilience points out, both recovery and learning are essential elements of cyber resilience [5,6]. The identity and access management (IAM) system provides the means for rebuilding the chain of trust upon which the restored services rely.

Table 2. Cloud IAM controls mapped to failure modes and resilience outcomes.

Control capability	Primary failure addressed	Resilience contribution	Saudi enterprise implication
Authoritative lifecycle automation	Orphaned and stale identities	Prevention and recovery	Connect HR, contractor, partner and workload events to cloud access
Phishing-resistant MFA	Credential theft and replay	Resistance	Prioritize privileged and high-impact services
Context-aware authorization	Compromised but valid credentials	Containment	Use device, location, risk and resource sensitivity in access decisions
Just-in-time privilege	Standing administrative access	Blast-radius reduction	Replace permanent admin roles with controlled elevation

Control capability	Primary failure addressed	Resilience contribution	Saudi enterprise implication
Federation assurance	Identity-provider or token compromise	Continuity and containment	Protect signing keys, restrict audiences, test provider outage
Identity telemetry and analytics	Anomalous sessions and entitlement drift	Detection	Normalize cloud identity events into enterprise monitoring
Automated revocation and rotation	Persistent attacker access	Response and recovery	Revoke sessions, rotate secrets and narrow access through governed workflows
Break-glass and restoration testing	IAM outage or lockout	Operational recovery	Protect emergency access and rehearse identity-service restoration

6 A governance framework for Saudi enterprises

The suggested framework views IAM as a resilience system covering the entire enterprise through six governance areas. The first of these is identity authority, which requires that every human and non-human identity have an accountable owner, an authoritative source, a lifecycle state, and a clearly defined relationship with business services. This avoids cloud directories becoming independent stores of outdated accounts. For Saudi organisations that operate across their subsidiaries, projects, and external partners, identity authority should be organised in a federated manner but be subject to the same lifecycle and assurance rules.

The second area concerns authentication assurance. Businesses must categorise their resources according to their business impact and then set appropriate authentication requirements based on that. Administrative, financial, industrial and personal-data functions which have a high impact should make use of stronger authentication factors and more stringent recovery procedures than those involved in low-risk collaboration. The aim should be proportional assurance, not as much friction as possible. Research into digital services in Saudi Arabia shows that security quality and user trust are linked; the controls had therefore to be both solid and easy to use [30]. Authentication programmes should assess enrolment integrity, the strength of the factors, abuse of the recovery mechanism, risky sign-ins, and the proportion of critical access that is protected by phishing-resistant methods.

The third area is authorization governance. Roles must be regarded as managed products having owners, purpose statements, the resources that are permitted, review dates, and separation-of-duties constraints. ABAC can be added to roles in order to make decisions that are sensitive to context, in particular when cloud resources span different business units or involve different data classifications. Wherever technically feasible, privileged access should be temporary. Access reviews should focus on high-risk entitlements rather than involve the carrying out of large certification exercises which are then mechanically approved by managers. This approach, which is based on risk, matches the amount of governance effort to the possible extent of the impact.

The fourth area concerns identity observability. Authentication, authorization, privilege, and federation events must be incorporated into security monitoring in order that identity-related incidents can be detected on various cloud platforms. The organization should specify a minimum telemetry set and a retention policy, but data collection must stay in proportion to its privacy responsibilities. Useful resilience measures are the mean time to revoke compromised access, the number of dormant privileged identities, the percentage of privileged sessions that are recorded, the

number of stale federation relationships, and the time needed to reconstruct critical access following an outage.

The fifth area concerns continuity and recovery. Since identity services constitute critical infrastructure, applications can become unavailable if authentication or federation fails. Business continuity planning should therefore involve providing redundancy for the identity provider, ensuring emergency administrative access, carrying out offline recovery procedures for important systems, making secure backups of the configuration, testing the restoration of directories and keys, and producing dependency maps for any applications that depend on central identity. Break-glass accounts must be strongly protected, kept under supervision, and regularly exercised in order that they will still be usable in an emergency and not end up becoming permanent bypass routes.

The sixth area concerns the integration of governance. The IAM architecture must link together cybersecurity, cloud governance, data protection, internal audit, human resources, procurement, and business continuity. This is especially significant in Saudi Arabia, since the country is rapidly adopting cloud services at the same time as its cybersecurity measures and its need for digital government services are becoming more established. Studies carried out in Saudi Arabia indicate that investments in security, levels of awareness, the technological infrastructure in place, and compliance with standards all have an impact on cybersecurity practices [2,29,30]. The enterprise IAM steering model should therefore convert regulatory and risk requirements into specific access-control outcomes rather than viewing compliance as a matter of producing documentation after deployment.

The implementation should take place in phases. In the first phase visibility is achieved by making an inventory of identities, privileged accounts, federation links, service principals, and critical applications. The second phase focuses on improving authentication and gets rid of any obviously excessive privileges. In the third phase lifecycle events are automated and privileged elevation is automated as well. In the fourth phase contextual authorization and continuous monitoring are introduced. In the fifth phase identity response is integrated with security orchestration and with continuity exercises. This approach prevents the usual error of buying advanced zero-trust tooling before the underlying identity data and ownership are reliable.

The framework also makes a distinction between maturity and resilience. Even if an IAM platform is technically advanced it can still be fragile should a single administrator, identity provider, or signing key constitute a catastrophic dependency. On the other hand, an organisation using simpler technology can be resilient provided that access is closely controlled, recovery procedures are tested and privileges can be quickly revoked. Saudi enterprises should therefore evaluate both control capability and failure tolerance; the aim should not be to achieve a completely trusted identity system but rather one that takes it for granted that mistakes and compromise will happen and is designed so as to reduce the length of time and the severity of their impact.

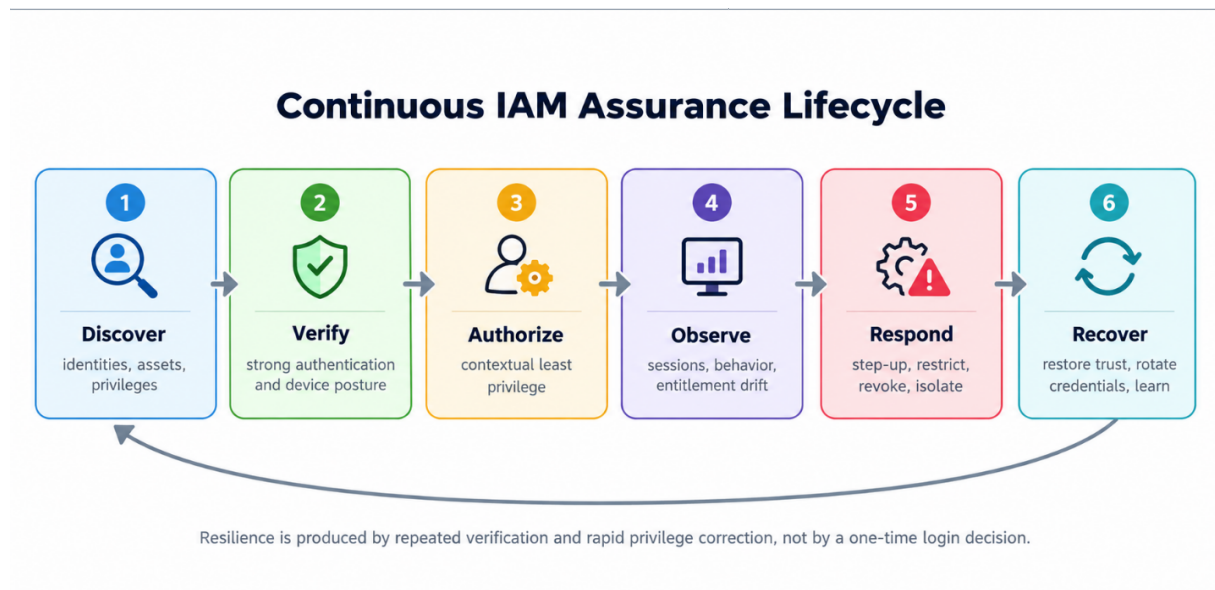


Figure 2. Continuous IAM assurance lifecycle: discover, verify, authorize, observe, respond and recover.

7 Discussion

The evidence leads to three main conclusions. Firstly, identity has now become the most stable kind of security boundary in a computing environment in which network location is becoming increasingly unreliable. The rise of cloud services, remote working, access by partners, and machine-to-machine communication all tend to blur the line between inside and outside. Since identities and privileges are still relevant no matter where a request comes from, IAM is able to offer a single level of decision-making across these different environments. Once again, network and endpoint controls are not eliminated; instead they can provide additional context for decisions based on identity.

Secondly, resilience arises as a result of interaction between control mechanisms. A mutual authentication framework even if it includes privilege governance can still allow excessive access following authentication. If least privilege is applied in the absence of accurate information about the lifecycle of identities, then inactive identities will still hold narrowly defined but nonetheless hazardous permissions. A zero-trust policy fails to adapt to changing risk levels if it does not have reliable telemetry. Centralized federation can lead to a single point of operational failure if there is no recovery plan in place. The most robust architectural approach is therefore one that is compositional in that the various aspects of identity lifecycle management, authentication, authorization, telemetry, response, and recovery must support and reinforce each other.

Thirdly, organizational governance is just as important as technical design. Zero-trust studies constantly name implementation complexity, cost, user experience, integration with legacy systems, and policy management as difficulties [7,8,12]. In the case of Saudi Arabia, the pace of transformation is rapid and it is necessary to link cybersecurity with business expansion rather than hinder it. The practical solution is not to loosen control, but to make control automated, based on risk, and measurable. Since identity, authentication, and authorization services can be reused, a well-designed IAM program can speed up digital delivery because applications do not have to rebuild these services from scratch.

There are still several tensions involved. While centralization enhances consistency it also raises the risk of concentration. Although greater telemetry improves the ability to detect problems it may at

the same time increase privacy exposure. Fine-grained authorization decreases the privileges of users but adds to the complexity of the policies. Short-lived credentials shorten the replay window but demand reliable automation. Strong authentication boosts assurance yet can harm usability if the recovery procedures and device enrollment are poorly designed. Because of these tensions, IAM maturity cannot be assessed simply by the number of features. Architecture decisions should be judged according to the extent to which they reduce possible attack paths while at the same time maintaining service availability and administrative recoverability.

The literature also shows a gap in measurement. Although a number of studies indicate technical feasibility or outline architectural advantages, fewer of them offer longitudinal evidence of the effect of IAM interventions on the frequency of incidents, on containment time, on recovery time, or on business disruption. This gap is especially important for enterprises in Saudi Arabia.

8 Research and practice implications

For those involved, the first thing they should do is ensure that identity risk is made clear. Businesses must set up a single, comprehensive list of workforce identities, privileged accounts, service principals, federation relationships, and important entitlements before carrying out more advanced policy automation. The security teams then need to focus on controls which reduce both the likelihood of an incident and its potential impact: these should include phishing-resistant authentication for high-impact access, just-in-time privilege, automated deprovisioning, session-aware monitoring, and tested revocation. Cloud projects should incorporate IAM threat modelling at the design stage so that identity dependencies are made explicit before the systems are put into production.

For researchers Saudi Arabia provides a valuable setting for empirical research since digital transformation is taking place at a high speed within the areas of government, finance, healthcare, industry, education and logistics. Future studies should compare the different sectors, assess zero-trust and IAM maturity in relation to measurable resilience outcomes, and look into how local regulatory requirements, the structure of the workforce, outsourcing arrangements and multi-cloud strategies affect the implementation process. Longitudinal case studies would be especially useful since the value of IAM tends to be seen in reduced exposure and quicker recovery rather than in immediate gains in productivity. Research should also look at non-human identity governance, privacy-preserving telemetry, and the resilience implications of concentration among identity providers.

9 Limitations

The review is constrained by the diversity of the evidence available. Studies of a technical nature, architectural proposals, surveys, and research into organizational matters each aim to address different questions and therefore cannot be regarded as directly equivalent. The group of thirty papers places a focus on work that has been verified through DOIs and may thus fail to include some valuable evidence from practitioners or publications that are not in English. Research into information and communication management (IAM) specific to Saudi Arabia is less extensive than that found in the international literature, which means that some of the technical conclusions have been taken from overseas studies and need to be validated in the local context. Lastly, the framework that has been proposed is only conceptual and must be tested using case studies tailored to specific

sectors, incident data, assessments of architecture, and long-term measurements of containment and recovery.

10 Conclusion

Cloud-based IAM can enhance an enterprise's cyber resilience if it is designed as a continuous control plane rather than merely as a set of login technologies. The review indicates that authoritative identity lifecycle management, strong authentication, granular authorization, resilient federation, continuous telemetry, rapid revocation, and trusted recovery all rely on one another. Although zero-trust principles clarify the architecture by eliminating implicit network trust, they only provide value when identity data, policy ownership, workload identities, and operational recovery are all mature.

For Saudi companies the strategic opportunity lies in incorporating these capabilities into the wider digital transformation linked with Vision 2030. The IAM system should link cloud architecture with cybersecurity governance, human-resource procedures, data protection, internal audit, incident response, and business continuity. The programmes must start with gaining visibility and establishing ownership before moving on to automated lifecycle control, contextual authorization, and identity-driven response. Success should be judged not just by the extent of authentication coverage but also by the reduction in privilege exposure, the speed of containment, reliable service recovery, and the proven improvement following incidents. In this approach, identity becomes the means by which digital growth and cyber resilience can both advance.

References

- [1] Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics*. 2022;11(1):16. <https://doi.org/10.3390/electronics11010016>
- [2] Saeed S, Altamimi SA, Alkayyal NA, Alshehri E, Alabbad DA. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*. 2023;23(15):6666. <https://doi.org/10.3390/s23156666>
- [3] Mostafa AM, Rushdy E, Medhat R, Hanafy A. An identity management scheme for cloud computing: Review, challenges, and future directions. *Journal of Intelligent & Fuzzy Systems*. 2023;45(6):11295–11317. <https://doi.org/10.3233/JIFS-231911>
- [4] Alsirhani A, Ezz M, Mostafa AM. Advanced authentication mechanisms for identity and access management in cloud computing. *Computer Systems Science & Engineering*. 2022;43(3):967–984. <https://doi.org/10.32604/csse.2022.024854>
- [5] Abdullayeva F. Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization*. 2023;12:100268. <https://doi.org/10.1016/j.rico.2023.100268>
- [6] Ferretti L, Magnanini F, Andreolini M, Colajanni M. Survivable zero trust for cloud computing environments. *Computers & Security*. 2021;110:102419. <https://doi.org/10.1016/j.cose.2021.102419>
- [7] Buck C, Olenberger C, Schweizer A, Völter F, Eymann T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*. 2021;110:102436. <https://doi.org/10.1016/j.cose.2021.102436>
- [8] Adahman Z, Malik AW, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security*. 2022;122:102911. <https://doi.org/10.1016/j.cose.2022.102911>
- [9] Syed NF, Shah SW, Shaghghi A, Anwar A, Baig Z, Doss R. Zero Trust Architecture (ZTA): A comprehensive survey. *IEEE Access*. 2022;10:57143–57179. <https://doi.org/10.1109/ACCESS.2022.3174679>
- [10] Xiao S, Ye Y, Kanwal N, Newe T, Lee B. SoK: Context and risk aware access control for zero trust systems. *Security and Communication Networks*. 2022;2022:7026779. <https://doi.org/10.1155/2022/7026779>
- [11] He Y, Huang D, Chen L, Ni Y, Ma X. A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*. 2022;2022:6476274. <https://doi.org/10.1155/2022/6476274>

-
- [12] Itodo C, Ozer M. Multivocal literature review on zero-trust security implementation. *Computers & Security*. 2024;141:103827. <https://doi.org/10.1016/j.cose.2024.103827>
- [13] Said W, Mostafa E, Hassan MM, Mostafa AM. A multi-factor authentication-based framework for identity management in cloud applications. *Computers, Materials & Continua*. 2022;71(2):3193–3209. <https://doi.org/10.32604/cmc.2022.023554>
- [14] Otta SP, Panda S, Gupta M, Hota C. A systematic survey of multi-factor authentication for cloud infrastructure. *Future Internet*. 2023;15(4):146. <https://doi.org/10.3390/fi15040146>
- [15] He H, Zheng LH, Li P, Deng L, Huang L, Chen X. An efficient attribute-based hierarchical data access control scheme in cloud computing. *Human-centric Computing and Information Sciences*. 2020;10:49. <https://doi.org/10.1186/s13673-020-00255-5>
- [16] Arshad H, Johansen C, Owe O. Semantic attribute-based access control: A review on current status and future perspectives. *Journal of Systems Architecture*. 2022;129:102625. <https://doi.org/10.1016/j.sysarc.2022.102625>
- [17] Wu Q, Li L, Zhang L, Mu Y, Rezaeibagha F. Secure and efficient general circuits attribute-based access control in cloud computing. *IEEE Systems Journal*. 2022;16(4):5533–5543. <https://doi.org/10.1109/JSYST.2022.3144730>
- [18] Chen E, Zhu Y, Liang K, Yin H. Secure remote cloud file sharing with attribute-based access control and performance optimization. *IEEE Transactions on Cloud Computing*. 2023;11(1):579–594. <https://doi.org/10.1109/TCC.2021.3104323>
- [19] Yan L, Ge L, Wang Z, Zhang G, Xu J, Hu Z. Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment. *Journal of Cloud Computing*. 2023;12:61. <https://doi.org/10.1186/s13677-023-00444-4>
- [20] Di Francesco Maesa D, Lisi A, Mori P, Ricci L, Boschi G. Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge. *Journal of Network and Computer Applications*. 2023;212:103577. <https://doi.org/10.1016/j.jnca.2022.103577>
- [21] Jalili V, Afgan E, Taylor J, Goecks J. Cloud bursting galaxy: Federated identity and access management. *Bioinformatics*. 2020;36(1):1–9. <https://doi.org/10.1093/bioinformatics/btz472>
- [22] Mikhaeil CA, James TL. Examining the case of French hesitancy toward IDaaS solutions: Technical and social contextual factors of the organizational IDaaS privacy calculus. *Information & Management*. 2023;60(4):103779. <https://doi.org/10.1016/j.im.2023.103779>
- [23] Wang R, Li C, Zhang K, Tu B. Zero-trust based dynamic access control for cloud computing. *Cybersecurity*. 2025;8:12. <https://doi.org/10.1186/s42400-024-00320-x>
- [24] Shen Q, Shen Y. Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach. *Computers & Security*. 2024;136:103537. <https://doi.org/10.1016/j.cose.2023.103537>
- [25] Schardong F, Custódio R. Self-sovereign identity: A systematic review, mapping and taxonomy. *Sensors*. 2022;22(15):5641. <https://doi.org/10.3390/s22155641>
- [26] Azad MA, Abdullah S, Arshad J, Lallie HS, Ahmed YH. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*. 2024;27:101227. <https://doi.org/10.1016/j.iot.2024.101227>
- [27] Fernandez EB, Brazhuk A. A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*. 2024;89:103832. <https://doi.org/10.1016/j.csi.2024.103832>
- [28] Aljumah A, Ahanger TA. Cyber security threats, challenges and defence mechanisms in cloud computing. *IET Communications*. 2020;14(7):1185–1191. <https://doi.org/10.1049/iet-com.2019.0040>
- [29] Aldahwan NS, Ramzan MS. Factors affecting the organizational adoption of secure community cloud in KSA. *Security and Communication Networks*. 2021;2021:8134739. <https://doi.org/10.1155/2021/8134739>
- [30] Al-Hawamleh AM. Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: Evidence from the KSA. *Digital Policy, Regulation and Governance*. 2024;26(3):317–336. <https://doi.org/10.1108/DPRG-11-2023-0168>
-