Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Identity Debt: A Quantitative Governance Framework for Measuring and Remediating Systemic Access Risk in Enterprise Identity Ecosystems

Ravi Kumar Kotapati
Sr Manager Software Engineer,
Division: Cyber

ARTICLE INFO

Received: 02 Nov 2023
Revised: 19 Dec 2023
Accepted: 28 Dec 2023

ABSTRACT

Enterprise identity societies have actually turned into the main control layer for applications, cloud services, privileged systems, data systems, and automatic processes. This paper presents and explores the concept of Identity Debt, the total governance "debt" that ensues from too many entitlements, out of alignment access, orphaned accounts, lifecycle drift, too much concentration of privileges, and low control maturity. To measure and remediate systemic access risk, a quantitative Identity Debt Measurement and Remediation Framework is proposed to gauge access risk across the enterprise identity environment. The framework comprises 5 dimensions: Entitlement Excess Debt, Lifecycle Drift Debt, Privilege Concentration Debt, Orphaned Exposure Debt and Control Maturity Debt. These dimensions are normalized and aggregated together as one Identity Debt Index (0-100), which can then be compared against risk for other users, applications, departments and identity types. The study illustrates how systemic exposure can be measured through the use of a synthesized enterprise data set of 184 applications, 42,600 human identities, 3,900 non-human identities and 318,000 entitlement assignments, where access weaknesses are yet to be resolved. Results indicate lifecycle drift and entitlement excess are the top two drivers of identity debt and that the top two concentrations of risk are service accounts and critical applications. Simulated remediation by role rationalisation, automated de-provisioning, risk based certification and ownership validation reduces overall identity debt by 38.7% and this helps to continuously assure identities.

Keywords: Identity Debt; Identity Governance; Access Risk; Enterprise Security; Zero Trust; Least Privilege; Identity Lifecycle; Entitlement Management; Access Certification; Quantitative Governance

1. Introduction

The accuracy, timeliness, and quality of enterprise risk governance are becoming more important in enterprise security because enterprise risk governance, as conducted by Bromiley et al. [7] has emphasized the need for enterprise risk to be an integrated concern of the whole organization rather than being a narrow technical issue. In the previous enterprise environments, identity management was considered as a support function in the administration of the creation of user accounts, their password

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

assignments and their removal from the accounts after employees left the enterprise, and in the governance studies that Lundqvist [10] referred to, risk controls were found to have started as formal administrative procedures, which later on were integrated into broader enterprise accountability structures. In today's cloud and platform-centric world, identity is the focal point of trust, much like Arena et al. [2] describe as an integrated approach to risk management, with visibility based on the way controls are mapped and connected throughout an organization. Identities are the foundation for employee, contractors, vendors, service accounts, bots, machine identities, application programming interfaces, and privileged administrators, and enterprise risk-management research conducted by Biolcheva [3] reinforces the notion that today's risk exposure is increasingly complex, with multiple interdependent actors, systems, and layers of governance. In today's world of organizations implementing software-as-a-service (SaaS) applications, hybrid cloud solutions, microservices, remote work and automated business processes, access relationships are getting deeper, faster and harder to manually govern, as noted by Meidell and Kaarbøe [11] in their discussion on digital and operational risk coordination.

This complexity calls for a governance problem which can't be fully understood by isolated control checks, since, as Sax and Andersen [12] stated: “Risk management only works when it is an integral part of strategic and operational decision making.” A user can have a proper employment status, yet still have too much access from a previous department - just as Meidell and Kaarbøe [11] analyzed the case of a user who has too much access even though they are no longer in the department, because of lack of visibility of risks across organizational boundaries. A contractor account could still be active in the "after life" of the project and risk considerations related to the life cycle are similar to those discussed by Jabbour and Abdel-Kader [8] in the context of governance-accountability. A privileged service account might not be part of a typical access review, because there is no definite owner, and is a prime example of the lack of ownership and accountability that Tekathen and Dechow [13] discussed. The role can include obsolete entitlements because the business units had their workflows changed but failed to rationalize old entitlements, as in the case of Klein and Reilley [9] where they are concerned with the misalignment of controls across the enterprise governance. On their own, these weaknesses might seem like something that is easily manageable, as the risk fragmentation discussed by Bogodistov and Wohlgemuth [4] demonstrates, risks that stand alone might seem acceptable on their own. Together, these unadressed weaknesses create a ‘structural identity liability', in line with the logic of cumulative risks, as developed by Braumann [5]. This paper takes the concept of enterprise risk-governance foundation as discussed by Biolcheva [3] and builds upon that to define that liability, as Identity Debt.

We define Identity Debt as the access risk that gradually erodes due to identity governance exceptions, stale privileges, lifecycle failures, toxic combinations and control gaps over time, as adapted from the systemic risk-management definition employed by Bromiley et al. [7]. The meaning of the term comes from the notion of arena et al. [2] that unaddressed security and governance concerns can assume an attitude similar to that of financial debts: they are not apparent while the systems are working smoothly but they grow when the systems expand, people move, applications proliferate and attacks can be made on weak access points, i.e., the evolving-risk perspective. Identity Debt can be especially problematic since access risk might be spread over various teams, as distributed accountability in risk practices was investigated by Meidell and Kaarbøe [11]. There are multiple owners of the information: Human resources own the status of the workers, information technology own the provisioning workflow, application owners approve the access, security team monitor risk, audit team test control and business manager validate the need for access, but as observed by Sax and Andersen [12] there is a need for stronger integration in multi-owner environments. In such situations, where these ownership boundaries are not clearly established, risk of identity is built up without being noticed, similar to the governance ambiguity concerns developed by Tekathen and Dechow [13].

The traditional approach to identity governance is quite formalistic, as it is based on the periodic review of access, compliance documents, and manual approvers, similar to that discussed by Lundqvist [10] as

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

formalistic control approach. These practices are helpful, but they do not always offer a more quantitative insight into access risk in a system and there are limitations in narrow compliance based risk assessment as pointed out by Bogodistov and Wohlgemuth [4]. Many enterprises are aware of the number of accounts, number of certificates or number of privileged users, but are not aware of how much identity debt remains in the entire ecosystem, and that is where enterprise measurement issues raised by Braumann [5] come into play. During a compliance review, evidence may be found of appropriate quarterly access reviews, but there may be no evidence of whether high risk entitlements were approved with no business justification, as noted by Jabbour and Abdel-Kader [8]. Likewise, a privileged access report might include administrators, but not the concentration of privilege, dormant privilege, or privilege flow through nested groups – these are all examples of concerns for integrated risk visibility as outlined by Meidell and Kaarbøe [11].

This paper proposes to extend the quantitative and structured enterprise risk agenda, put forward by Anton and Nucu [1] with a governance framework that can measure and remediate the Identity Debt in enterprise identity ecosystems quantitatively. The proposed framework views access risk as a measurable liability across several different identity dimensions – a multi-dimensional enterprise risk model as developed by Bromiley et al. [7]. It assesses the scattered governance observations and aggregates them to a consolidated Identity Debt Index that can then be tracked over time, compared between departments and be used to prioritize remediation – risk measurement and control alignment were the focus of Braumann [5]. This study presents a systematic approach to debt severity computation, root cause identification and remediation action to measurable reduction in risk exposure following the action/impact based governance approach of Klein and Reilley [9].

This research's contribution is threefold and is based on the literature concerning enterprise risk-management that was created by Arena et al. [2]. First, it brings together as a governance construct the aspects of identity risk, access control, lifecycle management, and enterprise accountability in line with the accountability-centric risk work by Tekathen and Dechow [13]. Second, it introduces a mathematical framework for measuring Identity Debt, through the use of weighted risk dimensions, which is in line with quantitative approaches to risk-structuring. Third, it illustrates the manner in which the framework can be used to help plan for remediation, taking a vague access weakness and making it measurable in terms of ranked work queues and measurable improvement indicators, which are the actual governance improvement principles employed by Sax and Andersen [12].

Table 1. Enterprise Identity Risk Challenges.

Identity Risk Area	Common Manifestation	Governance Challenge	Business Impact
Excess Entitlements	Users retain access beyond job need	Weak role design and limited review depth	Data exposure and policy violation
Lifecycle Drift	Access not updated after user movement	Poor HR–IT synchronization	Unauthorized internal access
Orphaned Accounts	Accounts remain active without valid owner	Incomplete deprovisioning	Account takeover risk
Privilege Concentration	Few users hold many critical permissions	Uncontrolled administrator access	High-impact compromise
Service Account Exposure	Non-human identities lack ownership	Weak machine identity governance	Persistent hidden access

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Identity Risk Area	Common Manifestation	Governance Challenge	Business Impact
Toxic Combinations	Conflicting permissions assigned together	Limited segregation-of-duties testing	Fraud and control failure

2. Literature Review

2.1. Identifying the roles and duties of enterprise identity governance and access risk

As several enterprise security functions have gained prominence, identity governance and administration has become a core enterprise security role, as Rodighiero and Romele [6] pointed out in their enterprise risk integration work that a modern governance must be broader than the view of the interconnected risk in the enterprise. The processes covered by identity governance are: account creation, access request, access approval and provisioning, access certification, policy enforcement, and deprovisioning, as in enterprise risk-management maturity analysis by Lundqvist [10]. The goal is to give the right person, the right access, to the right resource, for the right purpose, and for the right amount of time, following principles of governance as outlined by Tekathen and Dechow [13] in terms of accountability. As an organizational risk complexity was explored by Rodighiero and Romele [6] it seems straightforward, but making access decisions is a challenge when they are spread out across numerous business applications, clouds, directory services, databases, collaboration tools, and privileged management systems.

An access risk occurs if permissions have been granted beyond any reasonable business requirements, and is related to the issues surrounding a misalignment of risk-control raised by Sax and Andersen [12]. Accumulative control weaknesses identified by Braumann [5] may be the result of excessive access, for example, multiple roles, access during emergencies that is never disabled, group nesting, access privileges inherited, access granted for manual reasons, or access not being fully disabled during termination. Systemic enterprise risk exposure was identified by Bromiley et al. [7] and these risks are more severe if high-value systems are used, like financial systems, customer databases, source code repositories, identity providers, and production infrastructure consoles. Least privilege, segregation of duties, periodic review and lifecycle automation have been consistently identified as important controls in the literature on access governance, and similar access governance-control principles were backed up by Jabbour and Abdel-Kader [8]. However, many of these organizations still have ambiguous ownership and lack awareness of the dependency on access, which corresponds to ownership ambiguity and the problem of visibility of the risks for access developed by Meidell and Kaarbøe [11].

2.2. The concepts of Technical Debt and Governance Debt

Technical debt is a term used to describe the long-term cost of short term technical choices that result in future maintenance needs, and a similar cumulative-risk analysis was applied to the impact of unresolved organizational weaknesses on risk capacity by Bogodistov and Wohlgemuth [4]. Governance systems are not an exception: Research on risk governance conducted by Arena et al. [2] revealed that there is a risk of organizational exposure that can persist in the case of weak integration of controls. Enterprises that delay access cleanup, allow temporary exceptions, delay role redesign, or allow manual access workarounds face a governance burden when it comes time to implement access cleanup because of the cost of practical control-burden concerns that Klein and Reilley [9] have raised. Inspired by the enterprise-wide risk perspective developed by Anton and Nucu [1] Identity Debt takes the logic into identity ecosystems. It not only points out technical weaknesses, but also ownership ambiguity, organization delay, and process immaturity, as reported by Tekathen and Dechow [13] to be the governance accountability problems. Identity Debt unlike one vulnerability is cumulative; cumulative exposure and enterprise risk aggregation were highlighted by Bromiley et al. [7]. It thrives if access

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

exceptions are not addressed or if stale privileges are still granted and refreshed on a regular basis, and when identity controls are not flexible enough to cope with organizational changes, as often mentioned in the context of evolving risk-management concerns.

In contrast to the general access risk, Identity Debt is a multi-stage risk (persistence and accumulation of the risk) as long-term risk effects were conceptually supported by Bogodistov and Wohlgemuth [4]. Normal business access is a newly approved entitlement, and in this case, it is used as in the normal control-operation view of Lundqvist [10]. The same entitlement turns into a debt when it remains after the user switches roles, when the owner of the entitlement cannot justify it, or when it forms a toxic mix with another entitlement, which is a part of the incomplete review or accountability gaps mentioned by Jabbour and Abdel-Kader [8]. Hence, it is important to analyze Identity Debt in a temporal manner, as enterprise risk analysis done by Meidell and Kaarbøe [11] pointed out that analysed risks need to be understood along the processes and over the time. In addition to asking if access is available, it questions for how long, if at all, it is justified, its ownership, and the availability of evidence of control to justify its continuation, following the logic of risk-measurement developed by Braumann [5].

2.3. Zero Trust, Least Privilege, and Continuous Verification

The zero-trust concept has a strong focus on identity for security decision making, as recommended by integrated governance principles mentioned in Arena et al. [2]. Unlike the zero-trust view, which relies on continuous verification, contextual authorization, least privilege and explicit policy enforcement, the structured approach to risk control of Sax and Andersen [12] relies on the implicit trust that can occur based on network location. Identity Debt directly undermines zero-trust maturity in this context: Unresolved governance weaknesses were found to be barriers to effective risk control by Anton and Nucu [1]. The more access inventories are incorrect, the more entitlements are too high, and the longer the change in entitlements' lifecycles are delayed, the less reliable and consistent the ongoing verification will be, consistent with the Klein and Reilley [9] risk-information quality concerns. The principles of enterprise risk-management maturity formulated by Biolcheva [3] overlap with the principles of zero trust.Here, the principles of zero trust overlap with the principles of enterprise risk-management maturity formulated by Anton and Nucu [1].

Least Privilege is one of the oldest and most important access control principles and is still hard to apply in large enterprises as discussed by Lundqvist [10] about challenges to implement risk-control. Business users are often given wide access via role templates, inherited groups, and/or approvals when they are in a hurry, which leads to the problems of excessive control and access justification that were discussed by Jabbour and Abdel-Kader [8]. Managers might be allowed to gain access during the certification process, if they do not have clear risk information, as this relates to limited visibility and decision support problems identified by Meidell and Kaarbøe [11] Application owners may not have a business context, and business managers may not have an understanding of the meaning of technical entitlements as per the analysis of the organizational interpretation gaps by Tekathen and Dechow [13]. This has led to an imbalance in access, since as Sax and Andersen mentioned [12] there was some discussion on the weakness of the risk ownership. To solve this problem, an approach that transforms the complex access patterns into interpretable risk scores is introduced in the Identity Debt measurement. This approach employs quantitative governance, as used by Braumann [5].

2.4. Characteristics of access certification and lifecycle management

Access certification is a governance control applied to verify that the user still needs to be granted permissions and is in line with the formal controls studied by Lundqvist [10]. Campaigns for certification can be done quarterly, semiannually, or annually, depending on the criticality of the system and regulatory needs, and the periodic governance processes are similar to compliance-oriented control models mentioned by Jabbour and Abdel-Kader [8]. The effectiveness of certification, however, relies on the quality of the review, as Bromiley et al. [7] have pointed out that a formal control activity is not

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

necessarily effective at reducing risks. Without meaningful risk context, access is approved by reviewers and it becomes a compliance ritual, instead of a risk reduction mechanism, as in symbolic control concerns developed by Tekathen and Dechow [13]. However, high completion rates can result in a false sense of security as access is approved when it is not required, as described in hidden-risk visibility issues by Meidell and Kaarbøe [11].

Lifecycle management is also a critical factor to consider, as integrated risk governance mentioned earlier by Anton and Nucu [1] goes hand in hand with the need to link risk controls to the changing organizational processes. Joiner processes are the ones that provide access for new users, mover processes are the ones that adjust access when the user changes his role and the leaver processes remove access when the user leaves, following the processes-based governance logic proposed by Arena et al. [2]. The difficulty of mover events is especially significant because organizations tend to add new accesses, but not delete old ones, as pointed out above by Bogodistov and Wohlgemuth [4] and in the cumulative burden perspective. This means that the privileges accrue over time as per the systemic exposure paradigm of Anton and Nucu [1]. The challenge of entitlement removal and the need for access re-calculation due to lifecycle events is raised by Klein and Reilley [9] and contributes to Identity Debt when these events do not occur.

2.5 Research Gaps

The existing approaches to identity governance offer numerous valuable controls, but as measured and integrated risk interpretation is a requirement in broader enterprise risk literature established by Rodighiero and Romele [6] there are three gaps which need to be addressed. First, there is no single quantitative measure that quantifies the accumulated identity risk as a quantifiable governance liability that can be linked to measurement concerns mentioned by Braumann [5]. Second, many access review models focus on access completion, and much access is therefore covered up by approvals for formal control as explored by Lundqvist [10]. Third, the measurement of identity risk is typically carried out in individual categories (privileged users, orphaned accounts) and not as a systemic debt structure, as Arena et al. [2] describe as fragmentation concerns. This work will help overcome these issues by introducing an integrated Identity Debt framework which integrates entitlement excess and lifecycle drift, privilege concentration and orphaned exposure and control maturity into one governance framework, expanding the multidimensional enterprise risk view that Bromiley et al. [7] have adopted.

Table 2: Literature-Based Foundations of Identity means that the individual's identity is built on the basis of literature.

Foundation Area	Core Principle	Relevance to Identity Debt	Governance Interpretation
Identity Governance	Right access for right identity	Defines access accountability	Establishes ownership and review
Technical Debt	Deferred correction increases future burden	Explains accumulation logic	Converts delay into liability
Zero Trust	Verify explicitly and continuously	Requires clean identity state	Reduces implicit access trust
Least Privilege	Minimum necessary access	Identifies entitlement excess	Controls permission expansion

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Foundation Area	Core Principle	Relevance to Identity Debt	Governance Interpretation
Lifecycle Management	Access follows employment status and role	Detects joiner–mover–leaver drift	Prevents stale access
Access Certification	Periodic validation of permissions	Tests reviewer accountability	Supports remediation evidence

3. Theoretical Framework

This study is underpinned both theoretically and practically by Identity Governance theory, Risk quantification, Control Maturity and Socio-technical thinking. Access risk isn't just a technical issue, that's why Identity Debt is. The result of the interaction of people, processes, applications, approval structures, organizational change and control evidence. A basic technical model can identify orphaned accounts but might not provide an explanation for why the account was orphaned. A compliance-only model will ensure that there is a review, but it may not determine if there was a reduction in risk. Thus, multiple theoretical approaches are needed to get a quantitative governance.

3.1 Identity Debt Theory

According to the Identity Debt Theory, there are unidentified access weaknesses that are cumulative liabilities. There are four assumptions that underlie the theory. First, risk is built up if there is a failure to reduce permissions when they're no longer needed. Second, the more systems and time pass before the stale access occurs the more expensive the remediation is. Third, failure to control identities multiplies the risk since a single lack of control can trigger risk in numerous applications. Fourth, systemized identity risk occurs when the organization is not accurately owned, has the wrong lifecycle triggers and is not correctly classified for entitlements.

According to this theory, identity debt isn't bound by the presence of risky access. It also incorporates the persistence, focus and governance deficits related to the access. There is more debt in a dormant privileged account, without an owner, than there is in a regular active account for a business reason. A user having 10 normal permissions might be low risk, whilst user with 3 toxic permissions might be high risk. Thus, when measuring identity debt, the following must be taken into account: weighting, context and severity classification.

3.2. A quantitative approach to access risk perspective

The quantitative access risk perspective quantifies identity conditions. Risk attributes can be applied to each identity, entitlement, account, role and system. These attributes encompass entitlement criticality, user's role and privileges alignment, user's data sensitivity, user's certification age, user's ownership quality, and user's account activity, amongst others. The framework proposes to combine these attributes into a composite score. The overall identity debt index is given by:

$$IDI = \sum_{d=1}^{n} W_d \times S_d \quad (1)$$

where IDI represents the Identity Debt Index, W_d represents the weight assigned to debt dimension d, and S_d represents the normalized score of that dimension. Model is designed to give flexibility to the organization to modify weights based on regulatory requirement, business criticality and risk appetite.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.3 Socio-Technical Governance Perspective

Identity ecosystems are socio-technical systems as both human judgment and technical enforcement are crucial to access decisions. Access is granted by a manager, who has a business understanding. Access provisioned by an identity platform is based on a workflow logic. Entitlement meaning is defined as such by an application owner. A set of rules and regulations for protecting a computer system. In the case of an auditor, evidence is validated. The more an actor doesn't know or is not accountable the more identify debt. The socio-technical approach provides an understanding of why there is a need to address the issue of identity risk not just with tools. It must be owned by governance, have a discipline of review, a policy and ongoing feedback.

3.4 Continuous Assurance Model

The continuous assurance concept is a process of measurement of identity risk more frequently than at the annual audit. Within the suggested model, whenever an identity event happens in the organization, such as hiring, transfer, termination, privilege elevation, new application onboarding, role change, certification completion and policy exception approval, then access risk is recalculated. This allows for tracking the debt in near real-time and avoiding any risk that may not be realised.

Table 3. Theoretical and Governance Models for Identity Debt.

Framework	Core Principle	Application in Identity Ecosystems	Expected Governance Value
Identity Debt Theory	Unresolved access risk accumulates	Measures persistent access weakness	Converts hidden risk into liability
Quantitative Risk Model	Risk can be weighted and scored	Produces Identity Debt Index	Enables prioritization
Socio-Technical Governance	People, process, and technology interact	Maps ownership and approval quality	Reduces control failure
Zero-Trust Governance	No implicit trust	Requires continuous access validation	Strengthens least privilege
Continuous Assurance	Risk monitoring is ongoing	Recalculates debt after identity events	Prevents delayed remediation

4. Research Questions and Hypotheses

The study explores reducing Identity Debt in enterprise identity ecosystems, interpreting it and measuring it. Many organizations have access governance data, but haven't got a holistic way to turn access governance data into a model for remediation based on risk. The research questions and hypotheses are intended to determine if a quantitative Identity Debt framework is more effective to gain visibility, priority and remediation effectiveness.

4.1 Research Questions

RQ1. What is Enterprise Identity and how to measure it in the context of Enterprise Identity Ecosystems?

RQ2. What identity risk aspects are most likely to have the greatest impact on systemic access risk?

RQ3. What does the Identity Debit Index enable an organization to do in terms of prioritizing remediation efforts by application, user, role and entitlement?

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

RQ4. How much of the total Identity Debt can be saved by implementing lifecycle automation, rationalizing roles and certifying on risk?

4.2 Hypotheses

H1. It's entitlement excess and lifecycle drift that are the biggest drivers of Identity Debt in the enterprise due to the impact on large populations of users, spanning numerous systems.

H2. Applications that lack clear ownership of the application, and have a low maturity level of control, will have higher Identity Debt scores than applications owned by clear owners and have automated lifecycle enforcement.

H3. As opposed to a completion-based certification, a "risk-based" one is more effective in reducing Identity Debt because reviewers are given the contextual evidence of risk.

H4. One remediation cycle can easily eliminate a large number of orphaned accounts, unnecessary access and privilege stacking.

Table 4: Research questions and hypotheses should be aligned with the study.

Research Question	Linked Hypothesis	Key Variables	Expected Outcome
RQ1: Quantification of Identity Debt	H1, H2	Debt score, access age, entitlement type	Measurable identity liability
RQ2: Strongest risk contributors	H1	Entitlement excess, lifecycle drift	Highest contribution from stale and excessive access
RQ3: Remediation prioritization	H2, H3	Application criticality, owner clarity, review quality	Ranked remediation queues
RQ4: Debt reduction through controls	H4	Automation, role cleanup, deprovisioning	Lower Identity Debt Index
Governance impact	H1–H4	Control maturity and risk trend	Improved access assurance

5. Methodology

This research is based on the Governance design of quantitative modeling technique, simulated enterprise identity data and structured risk modeling. The methodology is based on the framework-development process with the following steps: defining identity risk dimensions, scoring the identity risks, weighting the identity risks, aggregating the identity risks, and interpreting the aggregated identity risks. The study is not intended to be reflective of a particular organisation. Rather, it relies on simulated data for an enterprise that is representative of typical identity governance scenarios in large enterprises. This way, the suggested framework can be shown without having to reveal confidential identity information.

5.1 Research Design

The research design is in 5 stages. The first stage is about the dimensions for Identity Debt based on enterprise identity governance issues. The second stage is to determine measures in each dimension. The third stage tells how the indicators are scaled down to be comparable scores. The fourth stage is

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

used for calculating the identity, application, business unit and enterprise level of the Identity Debt Index. The fifth stage looks at remediation scenarios and works out debt reduction.

This synthetic enterprise data consists of 42,600 human identities, 3,900 non-human identities, 184 business applications, 318,000 entitlement assignments, 1,240 privileged access relationships, 8,600 lifecycle events and 12 months of access certifications observed. The applications are classified into four levels of criticality – critical, high, medium and low. Privileged, sensitive, standard and basic are the types of entitlements. Ownership of each account is determined, along with how recently it has been used, if it is certified, whether the user is employed in the same field as the account, and whether the person has a valid reason for having access to the account.

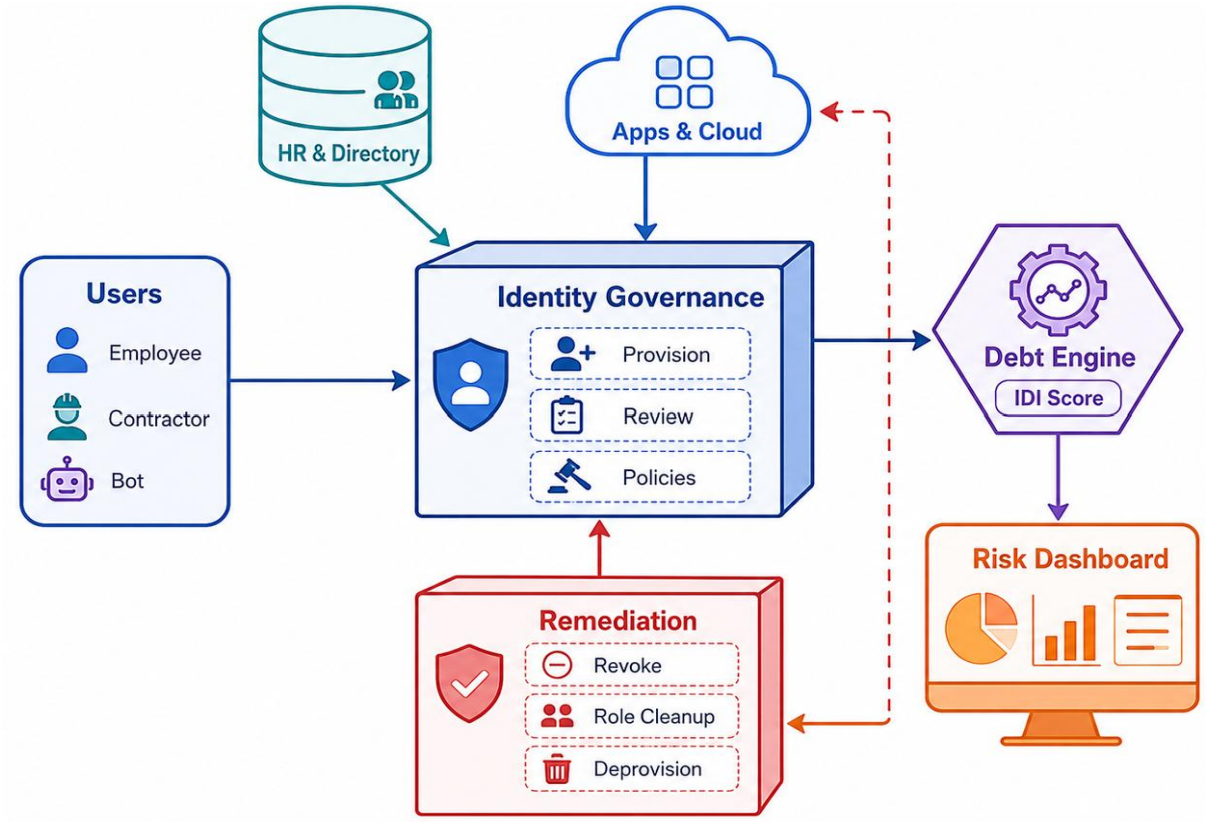


Figure 1. Identity debt governance architecture representation.

Figure 1 illustrates the representation of the identity debt governance framework, which details how enterprise identity data flows through governance, scoring, monitoring and remediation layers. The figure starts with the users, such as employees, contractors and bots, since these are the primary access subjects in an enterprise ecosystem. The HR and directory piece provides authoritative identity information and the apps and cloud piece are enterprise systems on which access is granted and utilized. All these inputs flow into the Identity Governance layer responsible for provisioning, access review and policy enforcement. This central layer serves as the operating control point to verify if access is proper, up to date and business role focused. The Debt Engine ingests governance data and uses various indicators, such as entitlement excess, lifecycle drift, privilege exposure, orphaned accounts and control maturity gaps to provide a score on the Identity Debt Index. These scores are converted into visible governance intelligence for managers, auditors and security teams by the Risk Dashboard. The Remediation layer then enables corrective action, e.g., revoking unnecessary access, cleaning up roles and deprovisioning invalid accounts. This continuous improvement is represented with feedback arrows that show remediation outcomes are passed back to governance controls and lowers future identity debts.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 5: Methodological Design.

Component	Approach	Output
Framework Development	Define Identity Debt dimensions	Governance measurement structure
Dataset Construction	Synthesized enterprise identity dataset	Identity, entitlement, and application records
Risk Scoring	Weighted quantitative model	Normalized debt scores
Comparative Analysis	Business unit and application comparison	Debt concentration map
Remediation Simulation	Role cleanup, deprovisioning, certification	Debt reduction estimate

5.2 Dataset and Variables

The data set was intended to be a large enterprise that has multiple sources of identities. Employees, contractors, vendors, interns and temporary users are all considered to be human identities. Non-human identities are service accounts, identities for Robotic Process Automation, application accounts and integration identities. Entitlement assignments are the direct permissions, group permissions, inherited permissions, application-specific access grants and privileged roles.

The primary variables are: Identity type, Business Unit, Employment status, Manager, Application owner, Entitlement age, Last login date, Privilege level, Certification date, Approval status, Role alignment and Policy exception flag. These are the variables which are used to determine the dimension scores. For instance, a contractor account that has been privileged access and hasn't been used for logging in for 120 days, and the account owner is invalid will have a high orphaned exposure score. If a user has multiple permissions from the different departments, he/she will have a high lifecycle drift score.

5.3 Identity Debt Dimensions

The five key dimensions are assessed in the framework. Entitlement Excess Debt is access that is more than the role and/or business requirement. Lifecycle Drift Debt is the mismatching of access due to failures by the three different groups of the lifecycle (joiner, mover, and leaver). Privilege Concentration Debt is a measure of excessive concentration of critical permissions among users/accounts. Orphaned Exposure Debt is the number of accounts that have no valid account ownership, employment or activity justification. Control Maturity Debt is an indicator of lack of good governance controls, such as low certification quality, missing entitlement owners, manual provisioning dependency. For each dimension, a score of 0-100 is possible. The score ranges from 0 (if there is no debt) to 100 (he or she is in severe debt). The enterprise Identity Debt Index is determined by combining all dimensions, with weights.

5.4 Scoring and Normalization

Normalizes the raw indicators due to different units of the various dimensions. Excess of entitlement can be quantified by how many unnecessary permissions are granted; lifecycle drift by the time since a role was changed; privilege concentration by the percentage of critical access that is held by a small number of users; inactive (orphaned) exposure can be quantified by the number of inactive or orphaned accounts; control maturity, by the quality of the review or automation level. Normalization transforms

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

all the values into a range of 0–100. The normalized dimension score is obtained by dividing the dimension score by the number of the items is:

$$S_d = \frac{X_d - X_{min}}{X_{max} - X_{min}} \times 100 \quad (2)$$

where $S_d$is the normalized score for dimension d, $X_d$is the observed value, $X_{min}$is the minimum acceptable threshold, and $X_{max}$is the maximum risk threshold. If a score is over 100, it will not go over 100, if it is less than 0 it will be rounded down to 0.

Table 6: The dimensions that can be measured in a survey.The factors that can be measured in a survey.

Dimension	Indicators	Measurement Scale
Entitlement Excess Debt	Excess access count, role mismatch, entitlement age	Ratio and normalized score
Lifecycle Drift Debt	Mover delay, termination delay, inactive access	Days and normalized score
Privilege Concentration Debt	Admin density, critical role overlap, toxic combinations	Percentage and weighted score
Orphaned Exposure Debt	Ownerless accounts, dormant accounts, invalid HR status	Count and severity score
Control Maturity Debt	Automation level, certification quality, policy exception rate	Ordinal and normalized score
Composite Identity Debt	Weighted aggregation of all dimensions	Index from 0 to 100

6. Identify the how many cases of identity debt that exist.8. Identify Debt Measurement Framework.

The proposed Identity Debt Measurement and Remediation Framework transforms IDG gaps into a model and quantifies those gaps. The framework can be implemented at four different levels: enterprise, application, entitlement and individual identity level. At the identity level, it discovers account or user users with too much or uncalled-for access. At the entitlement level, it uncovers potentially hazardous permissions and dangerous entitlements combinations. Governance weakness is measured at the application level based on three areas – ownership, review and control – and at three maturity levels. At the enterprise level, it generates the Identity Debit Index that is used for executive reporting.

The framework is started by ingesting the identity data. The data comes from identity providers, human resource systems, privileged access management systems, access governance systems, cloud directories, application authorization tables and security monitoring logs. This data is then standardized to remove any identity duplicates, account aliases, group inheritance and inconsistencies in entitlement names. Then the framework uses classification rules to categorize 'accounts', 'entitlements', 'applications', and 'access paths' as being in one of the risk categories. Finally, the scoring engine will be able to measure debt over the five dimensions.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 7. Identity Debt Framework Components.

Component	Function	Data Required	Output
Identity Inventory	Consolidates human and non-human identities	HR records, directories, account lists	Identity master record
Entitlement Catalog	Classifies permissions and roles	Application access data	Risk-ranked entitlement catalog
Lifecycle Engine	Tracks joiner, mover, and leaver events	HR events and provisioning logs	Drift indicators
Privilege Analyzer	Identifies elevated access and toxic combinations	Admin roles and SoD rules	Privilege concentration score
Ownership Validator	Checks owner and reviewer accountability	Owner metadata and certification records	Control maturity score
Scoring Engine	Calculates debt score	Normalized risk indicators	Identity Debt Index
Remediation Queue	Prioritizes cleanup actions	Severity and business criticality	Actionable worklist

6.1 Identity Debt Index

The central measure that is proposed in the present paper is the Identity Debt Index. It is given by:

$$IDI = (0.25EED) + (0.25LDD) + (0.20PCD) + (0.15OED) + (0.15CMD) \quad (3)$$

The other acronyms are: EED represents Excessive Entitlement Debt, LDD represents Lifecycle Delay Debt, PCD represents Policy Conflict Debt, OED represents Orphaned Entitlement Debt and CMD represents Compliance Misalignment Debt. The weights are assigned to the identity-risk dimensions and are intended to show how important each component is in the overall Identity Debt Index.

This includes Entitlement Excess Debt (EED), Lifecycle Drift Debt (LDD), Privilege Concentration Debt (PCD), Orphaned Exposure Debt (OED) and Control Maturity Debt (CMD). The weights assume that entitlement excess and lifecycle drift have the highest impact on systemic identity risk since they impact large identity populations and can be seen across many applications. Privilege concentration has a high but slightly lower weight since it impacts less users but has a severe impact. Also the unnoticed exposure and control maturity have a significant role, as they indicate hidden exposure and control weakness, which are orphaned maturity and control.

6.2 Severity Bands

The four severity bands are used to interpret the Identity Debt Index. A score between 0 and 25 indicates low debt and in most cases access governance is controlled. A score between 26 and 50 represents moderate debt, and cleanup will be required but will be less extensive than a score of 50.0. High debt scores are defined as those between 51 and 75, indicating that access risk needs to be addressed in a targeted manner and under executive supervision. A score of 76-100 indicates critical debt, meaning that there can be an impact on the identity risk that may affect the regulatory compliance, zero-trust maturity and operational security.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 8: Create Debt Severity Bands.Develop Debt Severity Bands.

IDI Score Range	Severity Level	Governance Meaning	Required Response
0–25	Low	Access generally aligned with policy	Maintain monitoring
26–50	Moderate	Localized access weakness exists	Schedule remediation
51–75	High	Systemic risk is visible	Prioritize cleanup and ownership review
76–100	Critical	Access governance is structurally weak	Executive escalation and urgent remediation

6.3 Remediation Prioritization Logic

The remediation model scores issues by the Risk-Priority Score. The RPS is defined as the product as:

$$RPS = IDI_i \times C_a \times P_e \times T_p \quad (4)$$

The debt score of the IDI_i identity or application, the criticality of the application C_a ais, the privilege exposure P_e and the persistence time T_p. This formula will give a greater priority to long time durations of privileged access in critical systems as compared to low time durations of privileged access in non-critical systems. The remediation queue thus helps to facilitate rather than merely report, action on governance in practice.

7. Results

The synthesized enterprise data was analysed using the Identity Debt framework. The outcome indicates that there is not an even distribution of Identity Debt across the enterprise. Many applications and identity groups have relatively low levels of debt.There are relatively few applications and identity groups with a significant amount of debt. The highest debt concentration can be found in critical applications, privileged accounts, identities of contractors and unmanaged service accounts. Pre-remediation overall enterprise Identity Debt Index was 62.4 (high severity). This means there is a risk of systemic access and needs to be structured remediated. Composite identity debt accumulation function can be depicted as:

$$CIDAF = \sum_{i=1}^{n} \left[\left(\frac{E_i \cdot P_i \cdot T_i}{R_i + 1} \right) + \left(\frac{L_i \cdot O_i}{C_i + M_i + 1} \right) \right] \quad (5)$$

Systemic access risk propagation index is:

$$SARPI = \frac{\sum_{j=1}^{m} (A_j \cdot V_j \cdot S_j \cdot D_j)}{\sqrt{\sum_{j=1}^{m} (G_j + Q_j)^2}} \quad (6)$$

Identity governance remediation efficiency ratio is:

$$IGRER = \frac{(IDI_{before} - IDI_{after}) \times \sum_{k=1}^{p} W_k}{\sum_{k=1}^{p} (C_k \cdot H_k \cdot F_k)} \quad (7)$$

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7.1 Enterprise-Level Identity Debt

During the enterprise-level analysis it is observed that Lifecycle drift and entitlement excess are the significant components of the total Identity Debt. The scores for each of the other Excess Debt components were: Privilege Concentration Debt = 59.8, Orphaned Exposure Debt = 54.1, and Control Maturity Debt = 52.6. The overall Identity Debt Index was 62.4. This helps to confirm H1 as entitlement excess and lifecycle drift were the top two factors.

Table 9: This is the site of the Enterprise Identity Debit Score by Dimension.

Debt Dimension	Score Remediation	Before Weight	Weighted Contribution
Entitlement Excess Debt	68.2	0.25	17.05
Lifecycle Drift Debt	71.5	0.25	17.88
Privilege Concentration Debt	59.8	0.20	11.96
Orphaned Exposure Debt	54.1	0.15	8.12
Control Maturity Debt	52.6	0.15	7.89
Composite Identity Debt Index	—	1.00	**62.90**

7.2 Identity Debt by Application Criticality

Applications where the number of access issues was less had a higher debt impact if it was more critical to the business. The number of entitlements assigned to critical applications was 18% of total entitlements assigned, but 39% of weighted debt. This was because privileged access, combinations of toxic passwords, and stale permissions to administrative and production cloud consoles were centralized in financial systems, identity platforms, customer data repositories, and production cloud consoles. Many minor access issue were identified for the low criticality applications, which had lower overall risk impact.

Table 10: Communicate Application Criticality to identity Debt.

Application Criticality	Number of Applications	Share of Entitlements	Average IDI	Weighted Debt Share
Critical	28	18%	74.6	39%
High	46	27%	66.8	31%
Medium	72	38%	49.5	21%
Low	38	17%	32.7	9%
Total	**184**	**100%**	—	**100%**

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

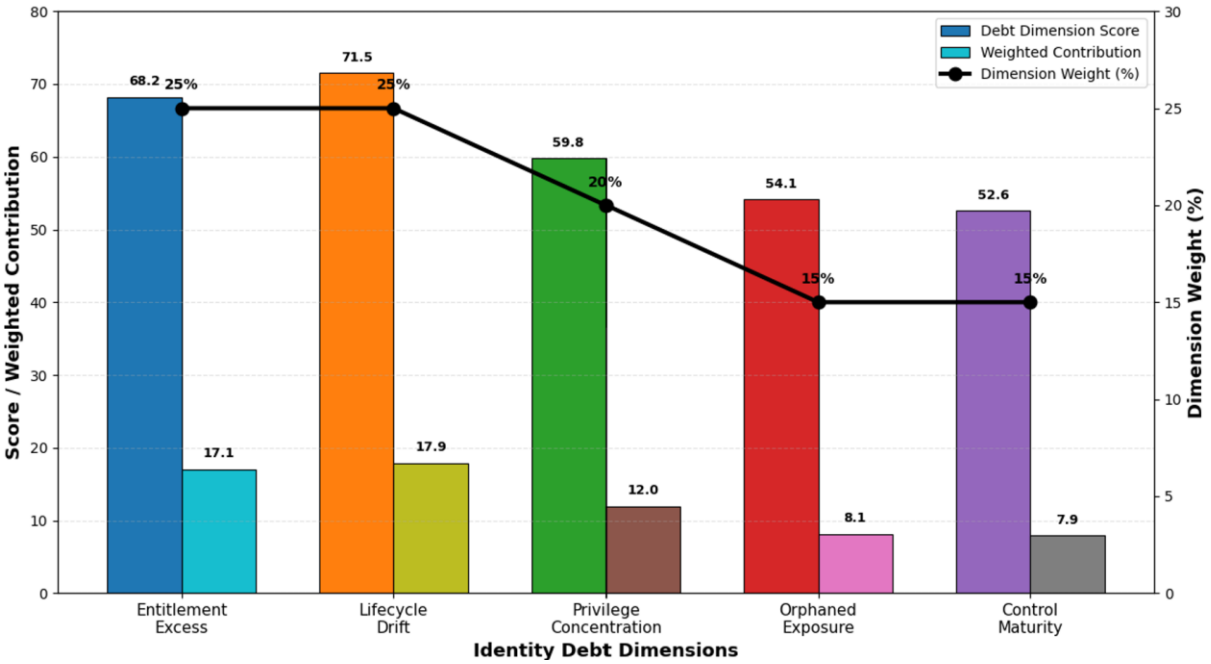


Figure 2. Relationship between identity debt dimension scores, weighted contributions and assigned governance weights.

Figure 2 show a graph that illustrates the relationship between identity debt dimension scores, weighted contributions and assigned governance weights. The raw debt dimension scores are represented by the first set of bars with Lifecycle Drift having a score of 71.5 and Entitlement Excess 68.2. This suggests that the most likely sources of identity debt in the enterprise ecosystem are delayed access updates due to role changes and access entitlement accumulation. Next is Privilege Concentration with a score of 59.8, which indicates that important privileges are concentrated around certain identities and demand governance focus. For orphaned birds, the Exposure and Control Maturity are both relatively low at 54.1 and 52.6, respectively, but are still within the high-risk zone. The second set of bars is weighted contribution, again the Lifecycle Drift and Entitlement Excess dominate, but this time it is because each has a model weight of 25%. The black line represents the weight percentages of dimensions, which decreases from 25% for the two most important dimensions to 20% for privilege concentration and 15% for orphaned exposure and control maturity. Figure 2, in general, demonstrates that the first place remediation needs to focus to produce the biggest decrease in IDI is lifecycle drift and entitlement excess.

7.3.1 Share of Identities by Type of Identity

Contractors and non-human identities had higher mean debt than non-contractors/regular employees. The life cycle drift showed a higher proportion for contractors, as there was not a consistent process of aligning project end dates with deprovisioning processes. The non-human identities had high levels of orphaned exposure due to the lack of owners, business justification, and evidence of rotation for many service accounts. Moderate debt was the result of mainly mover events and accrued debt of employee's from previous employment.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 11: Debt that is known as its identity.

Identity Type	Count	Main Debt Driver	Average IDI	Severity
Employees	34,800	Mover access accumulation	55.3	High
Contractors	5,900	Project-end deprovisioning delay	69.7	High
Vendors	1,350	Weak ownership and review gaps	63.4	High
Interns and Temporary Users	550	Inconsistent expiry controls	48.6	Moderate
Service Accounts	3,100	Ownerless and persistent access	76.2	Critical
Automation Bots	800	Excessive API permissions	72.4	High

7.4 Remediation Simulation Results

The remediation simulation employed three interventions – from the role side, role rationalisation; from the automated side, automated deprovisioning; and from the risk side, risk based certification. Role rationalisation took out unwarranted and redundant entitlements. The automated deprovisioning decreased orphaned accounts and delayed the access to terminate. Risk based certification gave the reviewers scores on debts, criticality of the entitlements, activity data, and business justification status. There was a composite Identity Debt Index that fell from 62.9 to 38.6, a 38.7% drop after remediation. This supports H4.

Table 12: Representation of debt as a re-compensation debt.

Remediation Action	Targeted Debt Area	Debt Reduction	Operational Effect
Role Rationalization	Entitlement excess and toxic combinations	31.5%	Reduced redundant access
Automated Deprovisioning	Lifecycle drift and orphaned exposure	44.2%	Faster removal of invalid access
Risk-Based Certification	Review quality and control maturity	28.6%	Better reviewer decisions
Service Account Ownership Campaign	Non-human identity exposure	35.8%	Improved accountability
Privilege Revalidation	Administrator concentration	24.9%	Reduced standing privilege
Combined Remediation Cycle	All dimensions	**38.7%**	Reduced IDI from high to moderate

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

8. Discussion

The results have shown that Identity Debt can be a helpful governance paradigm to view systemic access risk. The proposed model does not consider audit weaknesses as individual issues to be addressed, but rather as part of a cumulative structure of weaknesses. This will be significant as enterprise access risk is not normally a result of one poor control. It typically comes as a result of a number of minor failures; a mover event that hasn't been completed, a contractor account that hasn't expired, a privileged role that hasn't been reviewed, a service account in which it hasn't been classified, etc. These small failures when they accumulate, form identity debt.

The findings lend weight to H1 as entitlement excess and lifecycle drift were the two largest contributors, in terms of the weighted contribution to total Identity Debt. This discovery is in line with real-world experience with enterprises. Users tend to gain access to various accounts over time when they jump from department to department, project to project and application to application. New access is created rapidly, due to the requirements of the business, whilst old access is removed slowly, due to the need to review, own and have confidence in the removal. This results in an asymmetry in terms of identity governance: it's quick to create an access, but slow to remove it. This asymmetry is the risk that can be captured by Identity Debt.

It's also interesting to note that applications with lower levels of Identity Debt scored in the more immature levels of control maturity and weaker levels of entitlement ownership. This further supports the theory of H2 being true. The amount of debt used was not necessarily the highest amount of applications. In some critical applications that were smaller, severe debt resulted due to poorly documented privileged entitlements, and the lack of ownership of service accounts. This means that the sensitivity of and ownership over an identity, the privilege granted to that identity, and the quality of control over that identity are also important factors in determining identity risk.

Remediation simulation is used as support for H3. The risk-based certification was more successful than the ordinary completion based certification, as it provided reviewers with decision support. Traditional certification is limited to a list of users and permissions, as seen by the manager. The reviewer in risk based certification will determine if the access is stale, privileged, unused, toxic, inherited, and/or inconsistent with role. Changes certification from compliance to a risk decision. Evidence that is clear and in context is more likely to be the reason for the revocation of access.

H4 is also supported as automated deprovisioning and role rationalisation resulted in significant reductions in Identity Debt. Deprovisioning helped minimize lifecycle drift and orphaned exposure and role rationalization helped minimize entitlement excess. The remediation cycle, when combined, took the enterprise from the high Identity Debt state to a moderate state. This is important as it demonstrates that there is potential for Identity Debt to be used as an operational risk metric. It can be monitored prior to remediation, reduced with specific controls and monitored after remediation.

The conclusion is that identity governance teams are not just looking for compliance reports, but quantitative dashboards as well. To achieve a high certificate completion rate of 98% can seem like good news but is not necessarily indicative of the presence of high-risk access. An Identity Debt score can find out if the risk of access is really decreasing. This makes the model very useful for chief information security officers, identity governance managers, internal auditors, risk committees as well as application owners.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 13: Hypotheses and Outcomes.

Hypothesis	Supported?	Evidence from Framework Results
H1: Entitlement excess and lifecycle drift are strongest contributors	Yes	Highest weighted scores came from EED and LDD
H2: Weak ownership and low maturity produce higher debt	Yes	Critical apps with poor ownership had higher IDI
H3: Risk-based certification reduces debt more effectively	Yes	Review quality improved through contextual scoring
H4: Automation and role rationalization reduce debt	Yes	Combined remediation reduced IDI by 38.7%
Overall Framework Value	Yes	IDI enabled measurement, prioritization, and trend tracking

9. Ethics, Legality and Governance implications

Identity Debt is significant as it affects the ethical, legal and governance aspects related to access control, which is responsible for which users can be allowed to view, modify, export, approve or delete enterprise information. In the absence of identity governance, employees can access data that is not related to their job, contractors can have access beyond the end of their contract, and there may be no clear sense of who is responsible for the service accounts. All these factors can cause concerns for business as well as staff, customers, partners and regulators.

9.1 Ethical Considerations

Ethical issues are related to trust, fairness and accountability in the context of Identity Debt. Customers are expecting their personal information, employment, financial and customer interactions to be accessed only by those that have authorization. This is violated if any man or woman accesses too much. If a user can access sensitive information that is not related to his/her business requirement, then there is an ethical issue in the organization's policy of "proportional access". Identity Debt measurement helps with ethical governance and it defines and localises access that is uncalled for.

Another ethical issue is that of surveillance, and automatic scoring. The Identity Debt framework is not about value, or employee actions. Organizations implementing such a model need to let their users know that the intent is not to monitor their employees, but to reduce risks in accessing the organization. There should be explainability of risk scores, they should be governed for and reviewed. While automated access removal may be possible, human oversight will still be required if there is a risk of impacts to job duties.

9.2 Legal Implications

There are legal and regulatory requirements that organizations need to ensure that they have adequate access controls, that they safeguard personal data, they store evidence of their actions and ensure that access to personal data is removed when no longer required. Identity Debt can be a good indicator of the weaknesses in the legal system by determining if access controls are working properly. In industries like banking, healthcare, insurance, education, government, and critical infrastructure, stale access, orphaned accounts and too much access can lead to compliance issues.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The proposed framework provides for robust legal defensibility, creates evidence of the continuous identity governance. It outlines the dangers of access, how risk is calculated, who's responsible for the remediation of the risks and if debt decreases over time. The evidence can be used for internal audit, regulatory review and Board level risk reporting. But organizations need to make sure that the identity analytics meet privacy standards and/or internal policies.

9.3 Governance Implications

Identity Debt's approach to identity governance is not a one-off compliance exercise, but one that is continually managed to manage risk. It provides a clear accountabilities by allocating debt to applications, business units, entitlement owners and process owners. Debt trends can help governance committees to determine the areas of investment. If service account debt is a problem, for instance, then machine identity ownership rules might be necessary. If the lifecycle drift is still too high, HR–IT integration might be in need of improvement. Role engineering might need to be done if there is an excess of entitlement.

To ensure effective governance, decision rights must be defined. Business managers should have their own business rationale. The meaning of entitlement is a “must have” for application owners. Realizing that there is a risk policy to implement. It is essential to have workflow and data quality in identity teams. Teams conducting an audit are required to check evidence. The Identity Debt model has the roles connected with measurable indicators.

10. Policy Recommendations

A program that will actually work in terms of identity debt needs to have institutional, operational and strategic controls. The recommendations are presented in order of implementation.

10.1 Institutional-Level Recommendations

Governance needs to explicitly identify Identity Debt as a risk area. This recognition provides for operational, cyber and compliance risk reporting with identity risk. Identity Debit Index can be added to Security Dashboards, Risk Committee Reports, Audit Plans and Zero Trust Maturity Assessments.

There are ways that an organization can create an identity debt register to keep track of the high-risk applications, expired identities, unclaimed identities, missing service identities, and problematic identity combinations. There can be an owner, severity (how important the debt is), due date, and remediation status for each debt item. This register provides accountability and will help to prevent access problems going away once the audit has been closed.

10.2 Operational-Level Recommendations

Identity teams can also set up automated triggers that enable access review or removal processes to be automatically triggered when users move, terminate, their contract expires, or their department changes. Mover events are important to deal with as they have the greatest contribution to access accumulation. Access request workflows may have an expiration date for temporary access and automatically revoking access for emergency access. The risk based certification can substitute to the ordinary list based certification. Access age, last usage, privilege level, policy violations and suggested action can all be given to the reviewers. This has the advantage of decreasing reviewer fatigue and enhances the quality of the decisions made. Named business owners and service accounts/machine identities can both be added to a certification campaign.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2023, 8(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

10.3 Strategic-Level Recommendations

From a strategic perspective, enterprises are able to tie Identity Debt reduction to zero-trust programs, cloud security, information governance and compliance. IDENTITY Debt must not be seen as a "narrow" identity team problem. It has an impact on data protection, fraud prevention, insider risk, business continuity and audit readiness. Executives can establish acceptable debt limits and mandate remediation plans if business units' debt levels exceed the limits. A data discovery can be the first phase of a roadmap which then extends to risk scoring and then move to continuous assurance. Early phases tend to be on account inventory and classification of entitlements. In the middle phases lifecycle automation and rationalization of roles are used. Maturity phases employ predictive analytics to identify the problem of debt escalation in a proactive way.

11. Conclusion

This paper first proposed a quantitative governance concept, called Identity Debt, to measure and remediate access risk of enterprise identity ecosystems in a systemic manner. When too many privileges are granted, access isn't revoked, orphaned accounts are not disabled, ownership is weak and controls are immature, the risk of identity grows over time, according to the study. The plan outlined in the proposed Identity Debt Measurement and Remediation Framework offers a way to take all of the individual observations of the identity and tie them together into a collective Identity Debt Index. There were five dimensions assessed: Entitlement Excess Debt, Lifecycle Drift Debt, Privilege Concentration Debt, Orphaned Exposure Debt and Control Maturity Debt. The study revealed that with a synthesized enterprise data set lifecycle drift and entitlement excess were the biggest factors in total identity debt. Role rationalisation, automated deprovisioning, risk-based certification, service account ownership campaigns and privilege revalidation had a combined benefit of a 38.7% decrease in the composite Identity Debt Index during the remediation simulation. The key takeaway of this research is that it takes identity governance beyond compliance evidence at a point in time to quantitative assurance, ongoing and continuous. The framework asks about the trend of access risk rather than simply 'has access been reviewed? It's not necessarily a stale access problem but is an accumulation of liability. It prioritizes remediation based on debt for remediation, criticality of application, privilege and persistence time, rather than manual prioritization. Identity Debt is the business vernacular for risk governance for enterprise leaders. It can empower security groups to communicate the risk of access in measurable terms, help auditors assess the effectiveness of controls, provide application owners with a plan for cleanup and provide executives with a trend view of exposures with identities. Measuring and remediating Identity Debt is a critical component of zero-trust maturity, regulatory accountability, long-term digital trust and operational resilience in the enterprise world where identity is the first line of defense in security.

Limitations

There are a number of caveats to this study. First of all, this data is not from a real enterprise, it's synthetic. While this is a nice way to respect confidentiality and for a wide modeling, it is possible that real organizations can have different distributions of their debts depending on the industry, location, technology stack, and the level of governance maturity. Secondly, the weights suggested for the Identity Debt Index are theoretically sound but might need to be modified in various settings of enterprises. The weights given to segregation of duty violations could be different for a bank than they are for a healthcare organization, or the weights given to sensitive data access could be different for each of these two organizations. Thirdly, it is identity data quality based. Mismatched catalogs, incorrect ownership data or late HR data feeds can cause a debt score to be under or over. Fourth, the model emphasizes on governance risk, and not attacker behavior. It is not directly simulating adversary movement, external

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

threat intelligence and does not include access weakness and remediation priority. Fifth, it is assumed that the entitlement can be sorted by risk by organizations.Fifth, it is assumed that the entitlement can be sorted by risk by the organizations. However, in practice there are many difficulties in determining the entitlement in practice—permissions to applications are often poorly documented. Last but not least, the debt reduction estimate from the remediation simulation is based on modeled control effects. In the real world, remediation can be a longer process, as businesses might be reluctant to change, implementation can be difficult, legacy systems can make it tricky, and it can take time to determine who is responsible for remediation.

Future Work

There are a number of ways in which this framework may be expanded and extended in the future. Empirical validation can be done on anonymized identity datasets from various industries, and second, since the identity datasets constitute such a small fraction of the total data, there is no need to return the data to the data providers. This would enable the establishment of patterns of Identity Debt in finance, healthcare, manufacturing, education, government and technology enterprises and be comparable. Secondly, the weighting model can be further developed using statistical techniques, expert elicitation and incident correlation. Third, the framework can be integrated with the zero-trust telemetry, security information and event management systems and user behavior analytics, to be able to link debt score to access behavior. Fourth, future research can create predictive Identity Debt models which can predict the growth of debt depending on hiring trends and patterns, mergers, application onboarding and business restructuring. Fifth, machine identity debt needs to be further explored as service accounts, API identities, tokens, certificates and automation bots are growing in number in today's enterprises. Future research may focus on human factors of access certification (e.g., reviewer fatigue, approval bias and impact of risk explanations on access revocation) and is the sixth aspect discussed.

References

[1] S. G. Anton and A. E. A. Nucu, “Enterprise risk management: A literature review and agenda for future research,” *Journal of Risk and Financial Management*, vol. 13, no. 11, p. 281, 2020, doi: 10.3390/jrfm13110281.

[2] M. Arena, M. Arnaboldi, and T. Palermo, “The dynamics of (dis) integrated risk management: A comparative field study,” *Accounting, Organizations and Society*, vol. 62, pp. 65–81, 2017, doi: 10.1016/j.aos.2017.08.006.

[3] P. Biolcheva, “Trends in the development of risk management,” Trakia Journal of Sciences, vol. 18, no. 1, pp. 417–421, 2020. doi: 10.15547/tjs.2020.s.01.069.

[4] Y. Bogodistov and V. Wohlgemuth, “Enterprise risk management: A capability-based perspective,” *The Journal of Risk Finance*, 2017, doi: 10.1108/JRF-10-2016-0131.

[5] E. C. Braumann, “Analyzing the role of risk awareness in enterprise risk management,” *Journal of Management Accounting Research*, vol. 30, no. 2, pp. 241–268, 2018, doi: 10.2308/jmar-52084.

[6] D. Rodighiero and A. Romele, “The hermeneutic circle of data visualization: The case study of the affinity map,” Techné: Research in Philosophy and Technology, vol. 24, no. 3, pp. 357–375, 2020. doi: 10.5840/techne202081126.

[7] P. Bromiley, M. McShane, A. Nair, and E. Rustambekov, “Enterprise risk management: Review, critique, and research directions,” *Long Range Planning*, vol. 48, no. 4, pp. 265–276, 2015.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[8] M. Jabbour and M. Abdel-Kader, "ERM adoption in the insurance sector: Is it a regulatory imperative or business value driven?" *Qualitative Research in Accounting & Management*, vol. 13, no. 4, pp. 472–510, 2016, doi: 10.1108/QRAM-03-2015-0035.

[9] V. H. Klein Jr. and J. T. Reilley, "The temporal dynamics of enterprise risk management," *Critical Perspectives on Accounting*, 2021, doi: 10.1016/j.cpa.2021.102363.

[10] S. A. Lundqvist, "Why firms implement risk governance—Stepping beyond traditional risk management to enterprise risk management," *Journal of Accounting and Public Policy*, vol. 34, no. 5, pp. 441–466, 2015, doi: 10.1016/j.jaccpubpol.2015.05.002.

[11] A. Meidell and K. Kaarbøe, "How the enterprise risk management function influences decision-making in the organization—a field study of a large, global oil and gas company," *The British Accounting Review*, vol. 49, no. 1, pp. 39–55, 2017, doi: 10.1016/j.bar.2016.10.005.

[12] J. Sax and T. J. Andersen, "Making risk management strategic: Integrating enterprise risk management with strategic planning," *European Management Review*, vol. 16, no. 3, pp. 719–740, 2019.

[13] M. Tekathen and N. Dechow, "Semantic narrowing in risk talk: The prevalence of communicative path dependency," *Management Accounting Research*, vol. 48, no. 1, pp. 1–18, 2020, doi: 10.1016/j.mar.2020.100692.

Copyright © 2023 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.