PRACTITIONER REFERENCE · IDENTARA

The IAM Framework *Citation Gap*

What standards say vs. what practitioners think they say. The four ways an ISO or NIST citation parts ways with its source, and how to defend each one.

Vidyaa Ganesh Identara June 28, 2026

ABSTRACT

IAM practitioners rely on a small set of frameworks to defend their work, and the citations do not always match what the documents say. The mismatches are not confined to obscure corners. They appear on the controls teams are most confident about, where a reference to ISO or NIST diverges from the source. This paper maps how those citations fail, through four patterns observed in practice: the wrong concept, the wrong document, the stale edition, and the invented requirement. Each is worked against the primary source at a named edition, so the distance between what a standard says and what the field believes it says is visible. The paper then turns to application. It sets out how to defend each citation to an auditor, and it addresses the question every practitioner reaches, whether the frameworks can be relied on alone. They cannot, and the closing sections describe what carries the remaining weight once the citation is correct: the risk and architecture decisions the standards leave to the organization, and the evidence that a control is working. A reference table pairs the most-cited IAM concepts with the controls that ground them.

01 — Introduction

Citations travel faster than anyone reopens the source.

The frameworks are the backbone of how IAM decisions get defended. We cite ISO and NIST to justify a control to an auditor or to settle which practice a requirement calls for, and reading these documents closely is part of the job. Precise citation is still hard, for a structural reason: the documents are revised on their own schedules, and a citation passes from person to person faster than anyone reopens the source, so the wording in circulation can move away from the wording on the page. When that happens, the gap tends to surface in front of the auditor or client who knows the document best. This paper comes out of mapping the frameworks IAM teams cite most often, control by control, to find where the common citation and the source part ways.

Consider a claim that appears often in design reviews and audit responses: that a framework requires an authoritative source of identity, with identity proofing cited to support it. The instinct is right and the citation is wrong, and the reason is the subject of what follows.

The gap is between what the standards say about identity and access and what practitioners believe they say. It appears on the controls teams treat as settled, the access reviews and least-privilege rules that rarely send anyone back to the document, and that is what makes it costly. A miscited control clears design review and lands in policy long before anyone checks the source, by which point it is shaping how access is granted.

Across IAM work, these citations fail in a few recurring ways. Figure 1 maps the four this paper takes up, and the rest of the paper works each one against the source, then shows how to defend it and where the frameworks stop being enough on their own.

FIGURE 1 **The four ways an IAM citation fails.**

FAILURE TYPE	WHAT GOES WRONG	WORKED EXAMPLE IN THIS PAPER
Wrong concept	A requirement for one thing is used to justify another	Authoritative source argued from identity proofing
Wrong document	The right concept is cited to the wrong document in a family	Access rights argued from ISO 27001 when the guidance is in 27002
Stale edition	A rule from a superseded edition outlives the text that retired it	Password rotation, read as an ISO versus NIST conflict
Invented requirement	A specific rule is attributed to a standard that never stated it	Quarterly access recertification

02 — Why the frameworks matter

A shared language worth getting right.

The critique in this paper is meant to sharpen how the frameworks are used, and it helps to begin with what they provide.

They give the field a shared language. When everyone in a review points to ISO 27002 5.18, they are naming the same access-rights control, which is what allows a conversation about access reviews to take place. They carry hard-won consensus, since NIST SP 800-63 reflects years of research on what reduces identity risk, and its guidance on authentication is a shortcut past mistakes the industry has already paid for. And they travel: a control mapped to ISO or NIST can be explained to a regulator or a customer's security team, because those audiences already trust the reference.

None of this is in question. The value holds only when the citation is correct, and a good share of the time it is not.

03 — Scope and method

Each claim checked against the primary text.

This paper works the control-framework families that dominate IAM citation, each fixed to a specific edition.

NIST SP 800-53, Revision 5, through Release 5.2.0 (August 2025), the security and privacy control catalogue. **ISO/IEC 27002:2022**, the information security controls and their implementation guidance, read alongside **ISO/IEC 27001:2022**, which carries the requirements and the Annex A control list. **NIST SP 800-63-4** (final, July 2025), the digital identity guidelines, including the 800-63A, 800-63B and 800-63C volumes.

The scope is deliberate in two ways. COBIT and ITIL get miscited in IAM too, COBIT maturity levels read as access-governance requirements and ITIL practices read as access controls, but they belong to a separate piece, so the focus here stays on the ISO and NIST documents that come up most. Regulations sit outside the frame as well, since GDPR, NIS2, DORA and the EU AI Act impose obligations through law instead of describing controls, and treating a regulation and a control framework as interchangeable is its own citation error.

Every claim about what a standard says was checked against the primary text at the edition above and is cited to the control or clause. Where a concept is an architecture pattern rather than a stated requirement, the paper says so, since the line between a requirement and a practice derived from one is exactly where many citations slip.

04 — The wrong concept

Identity proofing answers a different question.

Begin with the first pattern, which is the most instructive of the four.

The claim is that a framework requires an authoritative source of identity, and the support offered is identity proofing. Identity proofing is the subject of NIST SP 800-63A, and it settles one question: whether a person is who they claim to be at the moment they enrol. It governs how a credential service provider validates a person's identity evidence and binds it to the applicant, and it grades the result as an Identity Assurance Level. Nothing in it speaks to whether your architecture maintains an authoritative system of record for identity data.

What makes the slip so easy is that 800-63A uses the words authoritative source itself, for something else entirely. Figure 2 sets the two meanings side by side.

FIGURE 2 Two meanings of “authoritative source.”

ASPECT	IN NIST SP 800-63A, IDENTITY PROOFING	IN IAM ARCHITECTURE
What it means	The issuing source of a piece of identity evidence, or a service with direct access to it	The enterprise system of record that owns identity data
Example	A motor vehicle agency for a driver's licence, the Social Security Administration for a Social Security number	An HR system feeding joiners and leavers into downstream provisioning
What it is for	Confirming during proofing that the evidence a person presents is genuine	Serving as the single source of truth that identities are provisioned from

The requirement an authoritative source answers to sits in identity management. ISO/IEC 27002:2022 control 5.16 states that the full life cycle of identities should be managed, with each identity uniquely tied to a single person or system, which is the basis for designating a source of truth for those identities. On the NIST side, account management in SP 800-53, control AC-2, governs how accounts are managed across their lifecycle and bound to authorized individuals. An authoritative source is the pattern that satisfies those requirements. So the justification that holds cites identity management and account management, and presents the authoritative source as the architecture that delivers them, instead of borrowing a proofing term that means something else.

The principle generalizes: before relying on a citation, confirm that the requirement being quoted addresses the concept being defended. Shared vocabulary is the most common way that check fails.

05 — The wrong document

27001 gets the credit, 27002 does the work.

Where the first gap swaps the concept, the second keeps the concept and swaps the document.

A common version of this claim runs as follows: ISO 27001 says to handle access rights this way, or NIST 800-53 requires identities to be provisioned like that. It sounds authoritative, and in IAM it usually points at the wrong document.

The two ISO standards behind every 27001 requires claim do different jobs. Figure 3 lays them out.

FIGURE 3 ISO/IEC 27001 versus 27002, on the same control.

ASPECT	ISO/IEC 27001:2022	ISO/IEC 27002:2022
Role	Names the requirement	Explains the implementation
What it contains	The management-system requirements and an Annex A list of 93 controls in four themes	Detailed guidance for each of those controls
What you cite it for	That a control applies to you, recorded in your Statement of Applicability	How the control is meant to work in practice
Example, control 5.18 Access rights	Listed as a control to consider	Worked out, with the provisioning and review guidance people quote

When a colleague cites 27001, control 5.18 for the specifics of how to run access reviews or shape a joiner-mover-leaver process, the obligation to have that control comes from 27001, but the guidance they are describing is pure 27002. The confusion is durable because organizations certify against 27001, so the certificate and the auditor's questions keep every access and identity control filed under that single number, including the parts that were always 27002.

In IAM this is not a harmless slip, because access controls are where audits concentrate. Naming the wrong document in an access review signals a citation made from memory, and an experienced assessor notices it immediately. The larger risk is that ISO 27001 requires us to recertify this way hardens into a mandate the standard never set, when the real obligations come from the risk assessment and Statement of Applicability, and a control listed in Annex A remains a candidate until the organization decides it applies to its identity estate.

06 — The stale edition

The password fight both standards already ended.

The third pattern is a matter of timing: a requirement from an older edition outlives the text that retired it.

Password rotation is the example practitioners reach for when asked where the standards disagree. The common account is that ISO expects passwords to expire on a schedule while NIST has prohibited the practice, leaving two respected frameworks in apparent contradiction. The account does not hold, because both standards have arrived at the same position.

NIST is the more straightforward of the two. Its SP 800-63B has pointed the same way since 2017, and the 2025 fourth revision hardened the point from advice into a requirement. The 2017 text said a verifier should not force scheduled password changes. Revision 4 says it shall not, and shall force a change only on evidence that the credential is compromised. The reasoning never changed: scheduled expiry pushes people toward weaker passwords and predictable edits, and buys little security for a lot of friction. The shift in wording matters when you cite this, because shall not is something an auditor can hold you to where should not was only guidance.

ISO is the half more often misremembered. Control 5.17 in ISO/IEC 27002:2022 contains no instruction to rotate passwords on a schedule. The triggers it names are tied to events rather than the calendar. Temporary credentials get changed at first use and vendor defaults at installation, and beyond that a password changes only when something happens to it, such as a confirmed compromise or a departure that leaves a shared credential live. The standard goes a step further in its own notes, observing that requiring frequent change can be counterproductive, since users faced with it forget new passwords, note them down in unsafe places, or choose unsafe ones, and it points to single sign-on and password vaults as the better path. That is the same argument NIST makes, sitting in the document people cite as NIST's opposite.

The conflict is a holdover from the previous edition. ISO/IEC 27002:2013 carried a password management control, 9.4.3, that did lean on periodic change, and the standard's own correspondence table shows 9.4.3 folding into today's 5.17. The expectation outlived the text: the 2013 control persists in circulation and gets attached to the current standard, and the result is read as a clash with NIST.

This is the citation gap in its clearest form: two frameworks in agreement, separated by an edition that no one reopened.

07 — The invented requirement

The quarterly rule no standard wrote.

The fourth gap adds to a standard rather than misreading one.

Asked how often access should be recertified, most practitioners answer quarterly. Asked where the requirement is written, no one can point to it, because no framework states it. The figure has the feel of something codified in the standards, and it is not.

ISO/IEC 27002:2022 control 5.18 calls for regular reviews of access rights and stops there. It sets no frequency. NIST SP 800-53 control AC-2 requires accounts to be reviewed, but on a frequency the organization defines for itself, a parameter the catalogue leaves open rather than a fixed interval. SOC 2 is the same story, principle-based, expecting periodic reviews with evidence and naming no interval. The one framework that does name a number is PCI DSS, which sits outside this paper's scope and reviews user access at least every six months, longer than the quarterly cadence everyone assumes. So quarterly is a convergent convention, the cadence teams adopt to stay defensible across whatever audit arrives. No IAM control framework states it. The error also appears in the literature, where framework comparisons sometimes attach a six-month or quarterly cadence to ISO 27001 that the standard never states.

This matters more than a pedantic correction, because the invented number crowds out the real question. If no standard sets the interval, the interval is yours to set on evidence, and the basis that holds up is risk. High-privilege, high-blast-radius access earns frequent review, and lower-risk access earns less, on whatever cadence your data supports. That is the argument of the companion paper, *Measuring What Moves*, which sets out how to drive recertification and other IAM decisions from metrics instead of habit. The gap here does more than name a wrong source: it lets that source stand in for a decision you should be making deliberately.

08 — Why these gaps persist

Citation in the field is largely oral.

None of this happens because IAM practitioners are careless. It happens because citation in the field is largely oral. A framework is learned from whoever onboarded you, or from an access-control matrix written several roles ago, and it passes along the way it was received. Even practitioners who know the documents inherit a shorthand for them, and it is the shorthand that carries into the next meeting and the next policy.

Two forces keep the shorthand in circulation. The first is version drift. Standards are revised on their own schedules, so a citation learned at one point can lag the current text by an edition or two. 800-63 reached its final form in 2025 and ISO restructured its access controls in 2022, and a reference picked up before those changes does not update itself. The second is name collision: similar-sounding documents and terms merge over time, the way 27001 blurs into 27002, or an authoritative source in proofing is read as an authoritative source in architecture. Together they produce confident citations to the right family and the wrong member, or the right idea and the wrong year.

09 — Validating a citation

A short check, before you rely on it.

The four gaps look different on the surface, but a single habit catches all of them, and it is not more memorization. It is a short check, applied before a citation is relied on or written into a policy. Figure 4 sets it out.

FIGURE 4 The check, before you cite.

01 **Name the document and the year.** ISO says and NIST says stop being citations the moment you remember that each name covers a family of documents across several editions.

02 **Open the source and read the clause at that edition**, whenever the point turns on specifics like the cadence of a review or whether an assurance level is mandatory.

03 **Check the kind of document you are holding.** Some standards list the requirement and leave the how to a companion, the way 27001 names a control and 27002 explains it. Others, like 800-63B, carry the detail directly.

04 **Apply the on-screen test.** If someone asked you to put the exact document and clause on the screen, edition included, could you do it, and would it say what you just claimed?

Reading the clause at its edition is what catches a borrowed concept, a wrong document, a retired rule and an invented one, in a single motion. Being able to answer yes to the last step is the difference between citing and repeating.

10 — Defending a citation

Using one in practice, and standing behind it to an auditor.

Applying a citation and defending it to an auditor are the same skill, because you apply a citation well by being able to defend it. An assessor rarely wants the control number alone. They want the number, the edition, and the evidence that you have done the part the standard left to you. A citation that names a clause but cannot answer the follow-up is weaker than no citation, because it signals a control that exists only on paper.

The pattern is the same across all four examples in this paper. State the claim, cite the document and clause that supports it, and be ready with the decision or the record the standard expects you to supply. Table 1 puts the four examples into those terms.

TABLE 1 From claim to citation to audit-ready.

THE CLAIM YOU MAKE	THE CITATION THAT SUPPORTS IT	WHAT AN AUDITOR WANTS BESIDE IT
We maintain an authoritative source of identity	ISO 27002 5.16 Identity management; NIST 800-53 AC-2 Account Management	The system named as the source of record, and how identities flow from it into downstream provisioning. Identity proofing, 800-63A, is a different control and does not support this claim.
We run access recertification	ISO 27002 5.18 Access rights; NIST 800-53 AC-2	Your defined review frequency, the risk basis for it, and the records showing the reviews happened. No standard mandates quarterly, so the basis has to be yours.
We enforce least privilege	ISO 27002 5.15 Access control; NIST 800-53 AC-6 Least Privilege	Evidence the principle is applied and reviewed over time, rather than set once when access was granted.
We do not force scheduled password changes	ISO 27002 5.17 Authentication information; NIST 800-63B	The event-based triggers you use instead, and confirmation that the current editions support removing periodic rotation, since an older edition did require it.

Handled this way, the citation stops being a quote and becomes a claim you can stand behind, which is the only kind that survives a review.

11 — Can you rely on the frameworks alone?

No, and the rest is yours to supply.

The answer is no, and it would be misleading to suggest otherwise. Correct citation is the floor on which the rest of the design stands.

A standard is written to be general on purpose. ISO 27002 tells you to manage the identity lifecycle and review access rights, and it does not configure your joiner-mover-leaver flows or decide how your platform

provisions. NIST 800-53 leaves frequencies and thresholds as parameters the organization sets, which is the whole reason no standard names a recertification cadence. The framework hands you the list of what to address. The decisions that turn the list into a working program are still yours.

Several of those decisions sit outside the text. Risk is the clearest case, because ISO 27001 is explicit that you select controls through a risk assessment and record what applies in a Statement of Applicability, so your risk posture decides how stringently you apply a control and which access you treat as high-stakes, while the clause itself stays silent on both. The standard leaves architecture to you as well, since an authoritative source or a least-privilege model is a pattern you choose to meet a requirement it states without drawing. Evidence is the part it cannot give you at all, because a control can be in place and still be ineffective, and no framework tells you whether yours is earning its keep. That last point is the subject of the companion paper, *Measuring What Moves*, which is why citation and measurement belong in the same conversation.

There is also a timing problem. Standards move on multi-year cycles, and identity practice does not wait for them. NIST did not name a control for identity providers and authorization servers until Release 5.1.1 in November 2023, years after teams were running them in production, and even then left IA-13 out of every baseline, so it stays optional. Treating the framework as the ceiling of good practice leaves the work a revision behind.

So the posture that holds is to treat frameworks as the shared language and the floor. Figure 5 shows the rest of what carries the weight.

FIGURE 5 **Frameworks set the floor. Read from the bottom up.**

LAYER	WHAT IT GIVES YOU	WHERE IT COMES FROM
Measurement	Evidence the control is working	The companion paper, Measuring What Moves
Architecture	The pattern that meets the requirement	Your design, chosen to satisfy what the standard states
Risk	Stringency, cadence, and which access is high-stakes	Your risk assessment and Statement of Applicability
Frameworks, the floor	A shared language and the list of what to address	ISO and NIST, cited to edition and clause

Frameworks are necessary, and were never built to be sufficient on their own. So cite them precisely, then add what they leave to you: the risk and architecture calls, and the evidence that the control works.

IAM concepts and their citations.

Table 2 pairs the IAM concepts that are cited most with the controls that ground them, and with the gap between what the standard says and what the field assumes. Citations refer to the editions listed in the scope section.

TABLE 2 **IAM concepts and where they are grounded.**

IAM CONCEPT	WHERE IT IS GROUNDED	WHAT THE STANDARD SAYS, AND WHAT PEOPLE ASSUME
Authoritative source of identity	ISO/IEC 27002:2022 5.16 Identity management; NIST SP 800-53 AC-2 Account Management	The standards require managing the full identity lifecycle and uniquely identifying each person and system. An authoritative source is the architecture that delivers this. The common error is to justify it with identity proofing, NIST 800-63A, which verifies a person at enrolment and is a different concept.
Access certification and recertification	ISO/IEC 27002:2022 5.18 Access rights; NIST SP 800-53 AC-2 Account Management	Both call for regular review of access rights, at a frequency the organization sets for itself. No standard in scope specifies quarterly or any fixed interval. The cadence is a risk decision the organization owns, and no standard dictates it.
Least privilege	ISO/IEC 27002:2022 5.15 Access control; NIST SP 800-53 AC-6 Least Privilege	A stated design principle, that everything is forbidden unless expressly permitted. The common error is treating it as a one-time provisioning setting rather than an ongoing rule for how access is granted and reviewed.
Password and credential management	ISO/IEC 27002:2022 5.17 Authentication information; NIST SP 800-63B; NIST SP 800-53 IA-5 Authenticator Management	Change credentials on first use, on vendor defaults, and on evidence of compromise. Neither current standard requires scheduled rotation, and 800-63B Revision 4 prohibits it outright. The rule to rotate every 90 days was retired with the older editions.
Multi-factor authentication	ISO/IEC 27002:2022 8.5 Secure authentication; NIST SP 800-63B at AAL2 and above; NIST SP 800-53 IA-2	MFA is required at higher assurance levels and treated as a strong control in secure-authentication guidance. The common error is a context-free mandate to put MFA on everything. The requirement tracks assurance level and risk.
Entitlement management	ISO/IEC 27002:2022 5.18 Access rights and 8.2 Privileged access rights; NIST SP 800-53 AC-3 Access Enforcement and AC-6 Least Privilege	The standards require provisioning and review of access rights, with tighter control over privileged entitlements. The common error is treating entitlement management as a product category rather than the implementation of these controls.

REF — References

Sources.

1. ISO/IEC 27001:2022, Information security management systems, requirements. Third edition, with Amendment 1:2024 on climate action.
2. ISO/IEC 27002:2022, Information security controls. Third edition.
3. NIST SP 800-53, Revision 5, through Release 5.2.0 (2025), Security and Privacy Controls for Information Systems and Organizations; control IA-13 introduced in Release 5.1.1, November 2023.
4. NIST SP 800-63-4 (2025), Digital Identity Guidelines, with volumes 800-63A on identity proofing, 800-63B on authentication and authenticator management, and 800-63C on federation and assertions.
5. Ganesh, V. (2026). “Measuring What Moves: A Dynamic Metrics Framework for Identity Governance Responsiveness.” Identara. Available at SSRN: https://ssrn.com/abstract=6842545 or https://doi.org/10.2139/ssrn.6842545