IDENTIVERSE 2026 . LAS VEGAS, NV . JUNE 2026

Identity Continuity Engineering

From Resilience Theory to Operational Practice

When identity fails: building resilience and recovery into your identity infrastructure

Shahan Karim Principal Architect

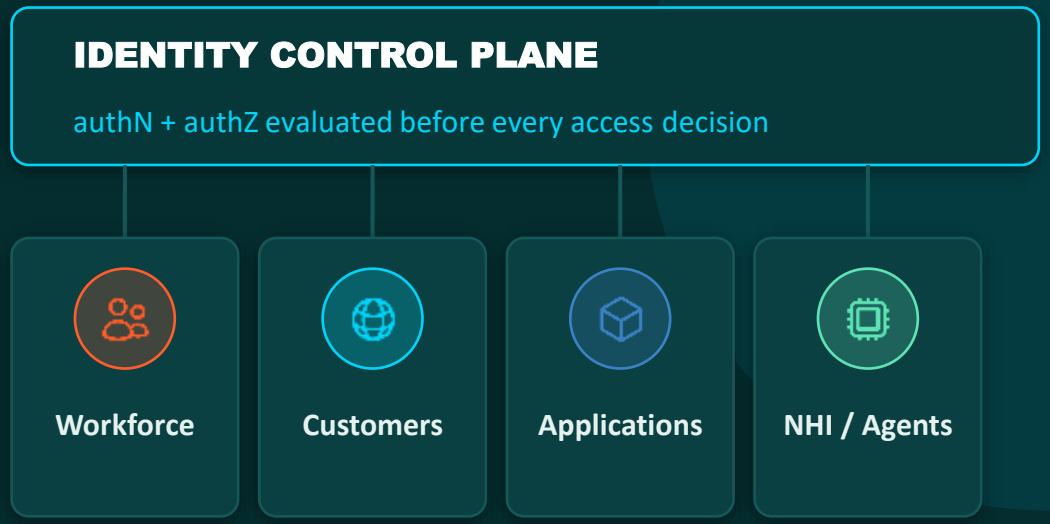
The system we depend on to restore control is the system whose failure removes it.

// WHY THIS MATTERS

Identity is now Tier 0 infrastructure

Every zero-trust access decision routes through identity first. When the control plane fails, every dependent class loses access simultaneously.

- Workforce productivity halts instantly
- Customer access is blocked at the front door
- Privileged admin is locked out at the worst moment
- Machine-to-machine flows fail before humans notice



Provider disruption cascades into operational paralysis

Three incidents in 12 months. Identity-layer failures, not compute failures. The pattern repeats regardless of vendor.

A major cloud IAM outage

A flawed automated quota update stripped permissions from IAM and 50+ core services. Consumer and enterprise apps went dark for ~7 hours. Identity was the single point of failure.

47 min — manual failover, one incident

An MFA provider outage

Authentication systems went offline for nearly 7 hours, locking Fortune 500 companies out of core business systems -- no backup auth path existed.

$8,600 — cost per minute of downtime

A global authentication degradation

142 engineers locked out of a single cloud region at one organization. Manual failover took 47 minutes because no automated identity failover mechanism existed.

>$400K — direct cost, one incident

Optimized for prevention -- not continuity

Three assumptions embedded in modern identity architecture -- all three break under disruption.

It will be reachable

Cloud concentration, network failure, or tenant compromise make the control plane unavailable exactly when it's needed most.

Available = resilient

A service can be up yet unusable -- policy corrupted, admins locked out, or cryptographic trust you can no longer verify.

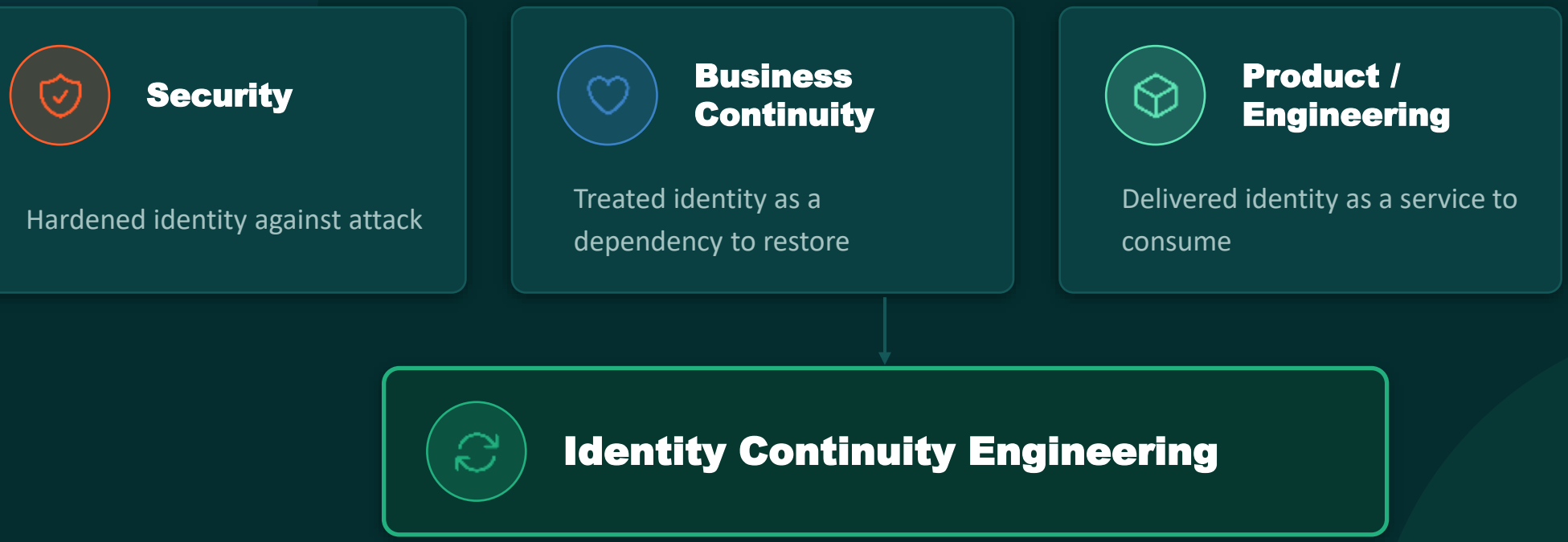
Human IAM is separate

Workload and agent identities now outpace human accounts and break first -- before any person notices a problem.

Zero trust improves security posture -- but deepens dependence on centralized policy evaluation if continuity is not designed in from the start.

Identity continuity engineering: the missing discipline

The three silos that have defined digital identity must collapse into a single engineering discipline.



Seven lessons from enterprise implementations

identiverse

Drawn from large-scale identity resilience implementations across hybrid and multi-cloud environments.

1 **Recovery inside the thing you're recovering is not recovery --**

Break-glass in the primary directory, recovery playbooks behind the primary IdP -- fail precisely when needed. IRIP must be genuinely isolated.

2 **Non-human identities break first and loudest --**

Machine-to-machine stops immediately; humans coast on cached tokens. NHI is first-class, not an afterthought.

3 **Testing is the only proof --**

Untested recovery fails at >60% when first exercised. The gap between documented procedures and operational capability is consistently larger than expected.

4 **Hybrid sync is the silent killer --**

Split-brain is harder to diagnose than outages and can persist undetected for hours, compounding incident recovery.

5 **The application layer is where resilience dies --**

Apps hardcoded to one issuer bypass infrastructure-layer resilience entirely. App-layer continuity must be tested in every exercise.

6 **Identity resilience is a team sport --**

Security, infrastructure, application, and business continuity must all be in the room. No single team owns all the context.

7 **Start with break-glass, expand from there --**

A simple, well-tested break-glass is the fastest path to value and the foundation all other resilience layers build upon.

PART ONE

The Foundation

12 Modern Identity Laws

Evolving Kim Cameron's Laws of Identity for the decentralized era. Four are the direct operational foundation of continuity & resilience.

01 Self-Sovereign Identity	**02 Decentralization**	03 Privacy	04 Security
05 Transparency	06 Attestations	07 Equity	**08 Interoperability**
09 User Control	10 Data Minimization	**11 Data Portability**	12 Auditability

Laws 01, 02, 08 & 11 are the four resilience primitives -- all 12 at IdentityLaws.com

I wrote the resilience case three years ago

Each of the four highlighted laws has a direct operational reframe when applied to identity continuity.

LAW 1

Self-Sovereign Identity

If the user holds the credential, the IdP outage does not destroy the identity. A VC in a wallet is verifiable offline -- no live connection to the issuer required.

LAW 2

Decentralization

"Decentralized systems can be more resilient -- they do not have a single point of failure." Written in 2023. The 2025 incidents proved it.

LAW 8

Interoperability

You cannot fail over from IdP A to IdP B if your application is hardcoded to one vendor's SDK. Interoperability is the prerequisite for continuity.

LAW 11

Data Portability

Identity state must be portable between providers. If tokens, sessions, and credential metadata cannot move -- failover is architecturally impossible.

PART TWO

The Four-Layer Framework

Four layers of identity continuity

Bottom = what organizations have today. Top = true continuity. Climbing the stack means less dependence on any single provider.

LAYER 4

Application-Layer Continuity

Degrade gracefully; accept multiple issuers; cache trust at the application

LAYER 3

Sovereign Resilience

Verifiable Credentials verified offline -- identity survives total provider failure

LAYER 2

Federation Resilience

Multi-IdP + dynamic trust resolution; fail over between providers

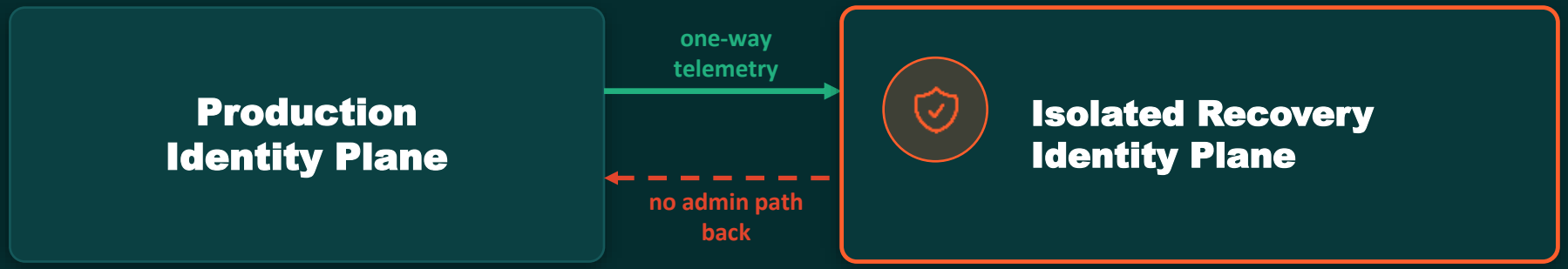
LAYER 1

Infrastructure Resilience

Isolated Recovery Identity Plane, outside the blast radius of the primary

Isolated Recovery Identity Plane (IRIP)

If recovery depends on the system being recovered, the plan is circular -- and fails under exactly the conditions it was built for.



- Isolated identity authority
- Scoped cross-boundary admin
- Federated identity bridging
- WORM telemetry store
- Break-glass operating mode

Multi-IdP architectures & dynamic trust

Layer 2 addresses provider-level failure: what happens when the identity provider itself is unavailable?

Backup IdP

A secondary provider mirrors policy and users. On outage, apps redirect. Cold-start latency is the main risk to manage.

Split IdP

Two providers run concurrently. User base distributed across both -- eliminating cold-start at the cost of higher operational complexity.

OpenID Federation 1.1

Final Specification -- May 2026

Trust chains without bilateral agreements. An app can discover and trust a backup IdP through federation trust infrastructure -- no pre-configured point-to-point integration.

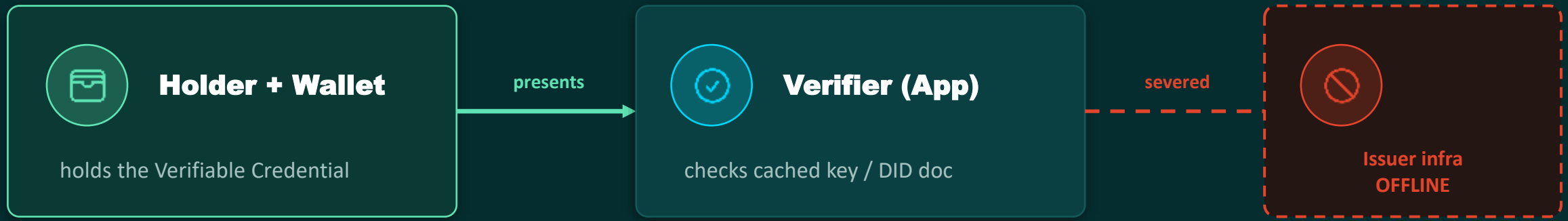
REQUIRES ?

- **Provider-neutral identity state**
- **Synchronized policy configs**
- **Health-check IdP selection**
- **Tested failover drills**
- **Identity-specific RTO / RPO**

Better than Layer 1 alone -- but still assumes centralized providers are available to serve as the backup.

Identity that survives total provider failure

A Verifiable Credential is validated with only the issuer's cached public key. No live connection to the issuer required -- ever.

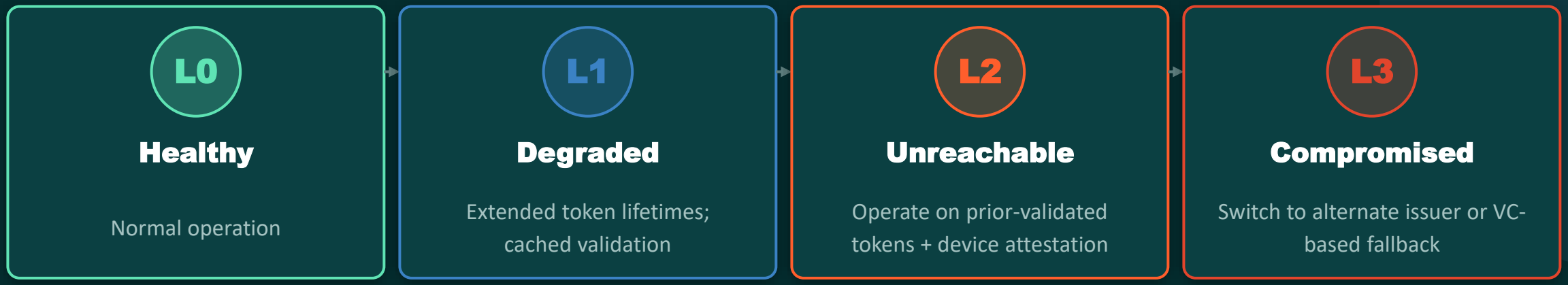


- Issue VCs alongside tokens for critical identities
- DIDs decouple identity from any single registry
- Cache JWKS / DID Docs at the application layer
- VC-based break-glass for admin recovery

Where resilience dies: the application layer

No OIDC or OAuth 2.0 spec defines how an application fails over between providers. Even perfect IdP failover fails if the app can't switch issuers.

PROGRESSIVE DEGRADATION MODEL



Proposed standards extensions . fallback_issuers in .well-known/openid-configuration . RFC 8693 token exchange for provider switching . application-side JWKS cache . VC fallback

Identity resilience must become a protocol feature -- not a vendor feature.

Automate recovery -- govern machine identities

Manual failover doesn't scale. Non-human identities break first. Both require engineering-grade automation.

SOAR Identity Playbooks

Automated lockdown, credential rotation, and IdP switchover in minutes. Identity incidents trigger pre-defined cross-team workflows.

Synthetic-Auth Monitoring

Test logins every 60 seconds. Detect degradation in seconds, not hours. Cover: availability, trust integrity, cert expiry, federation chain health.

Identity Chaos Engineering

Intentional failure injection -- IdP outages, cert expiry, sync corruption -- to measure actual recovery time against targets.

SPIFFE / SPIRE for Workloads

Attestation-based workload identity. Short-lived X.509 SVIDs rotate continuously and federate across cloud trust domains. CNCF graduated.

Regulators are converging on resilience

Despite different legal language, the same five themes emerge globally. Identity sits at their intersection.

DORA

ICT third-party & concentration risk. Article 29 requires substitutability assessment. The top 3 cloud providers support >70% of EU financial cloud infrastructure.

NIS2

Extends to energy, transport, health, water, digital infrastructure. Management accountability, supply-chain security, incident reporting.

NIST SP 800-63-4

Continuous risk management replacing one-time assessments. Digital wallet integration. Subscriber-controlled wallets recognized in the federation model.

FIVE CONVERGING GLOBAL THEMES

- **Critical ops must survive disruption**
- **Third-party concentration must be governed**
- **Boards are accountable**
- **Recoverability must be tested**
- **Evidence matters**

Resilience must become a protocol feature

Current specs were designed for security and interoperability -- not continuity. Vendor SDKs fill the gap but create vendor lock-in for resilience itself.

OIDC / OAuth 2.0

Assumes a single, available authorization server -- no failover behavior defined

SAML

Bilateral trust relationships -- no failover mechanism of any kind

OpenID Federation 1.1

Dynamic trust resolution -- but no failover behavior specification

W3C VC 2.0

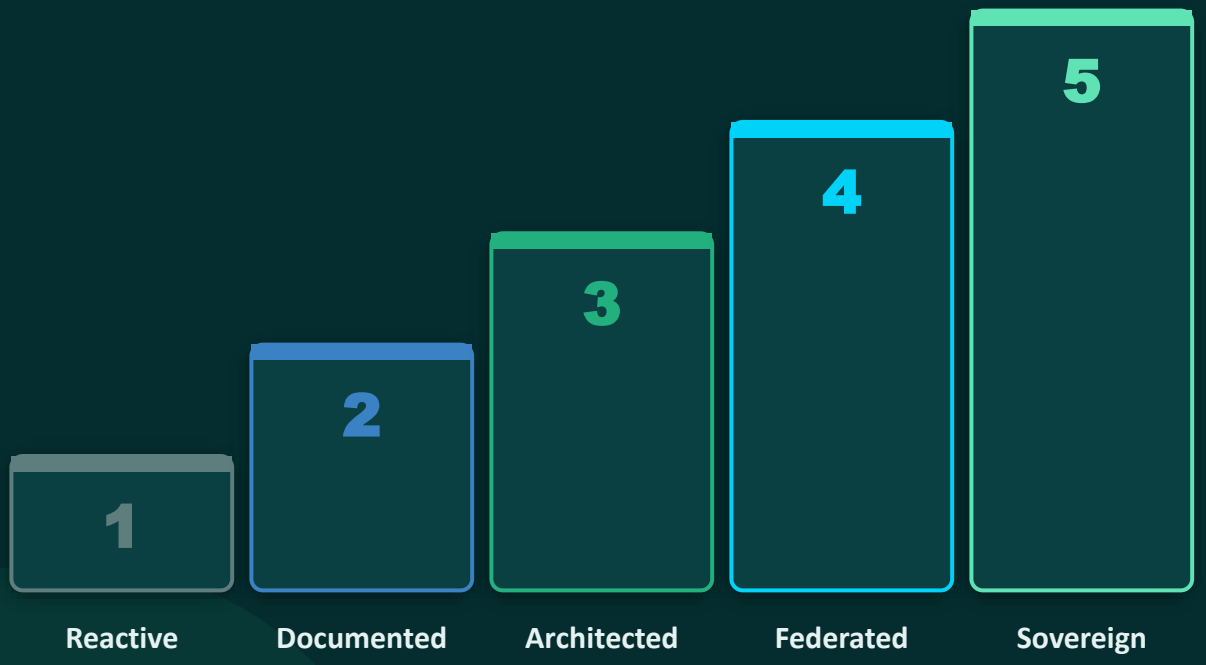
Offline verification -- but no enterprise fallback authentication integration

The call to the identity community

The IETF, OpenID Foundation, and W3C must define a formal Identity Continuity Specification: discovery failover, token exchange for provider switching, progressive degradation, and VC-based fallback authentication integration.

From Reactive to Sovereign

Most teams think they are Level 2 because they have strong IAM. Most are actually Level 1 -- they cannot prove continuity under disruption.



RTO ? MATURITY LEVEL

Identity RTO > 4 hours	**Level 2**
RTO 1-4 hours	**Level 3**
RTO 15-60 minutes	**Level 4**
RTO < 15 minutes	**Level 5**
DORA / NIS2 regulated	**Level 3 min.**

Measure continuity -- not just availability

Traditional SLAs measure provider uptime. These KPIs measure enterprise continuity of trusted access.

MTIDR

Mean Time to Identity Recovery

Measured average from detection to full restoration. Compare against RTO targets quarterly.

Auth Success

During Degradation

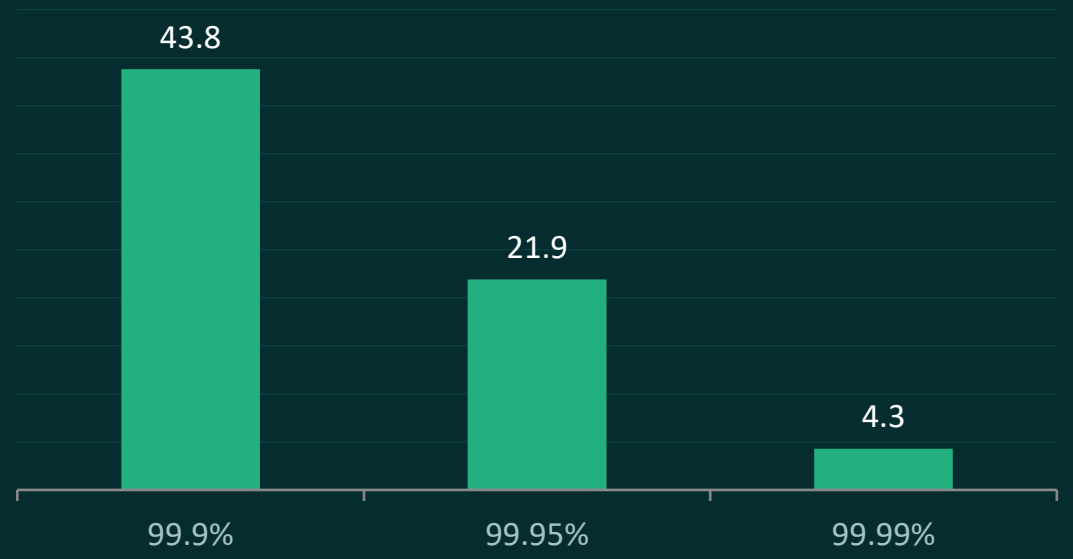
% of auth attempts that succeed during disruption. Target ? 95% in planned failover scenarios.

RTO / RPO

Per Access Class

Defined separately for workforce, privileged, NHI, and customer auth -- each has a different business impact profile.

MAX DOWNTIME (MIN/MONTH) BY AVAILABILITY TIER



At 99.99%: 4.3 minutes/month. Identity must be held to Tier 0 standards.

Report identity uptime as a board KPI -- tied to revenue impact, not buried in security operations.

CONCLUSION

Identity continuity engineering needs to become a first-class operational capability

When the user holds the credential, and the credential is cryptographically verifiable without a live connection to the issuer, identity reaches a level of resilience that no amount of infrastructure redundancy can match.

The building blocks exist today: OpenID Federation 1.1 . W3C Verifiable Credentials 2.0 . SPIFFE/SPIRE . NIST SP 800-63-4. What remains is the engineering discipline -- and the standards work -- to make identity resilience a protocol feature, not a vendor feature.

Shahan Karim

APPENDIX

Reference Slides

Additional detail for Q&A -- nothing has been discarded from the original deck

You cannot go full sovereign overnight

Three horizons -- actionable at every maturity level. Start with break-glass. Expand from there.

TODAY

0-6 months

- Map all Tier 0 identity dependencies + single points of failure
- Stand up an Isolated Recovery Identity Plane + break-glass accounts
- One-way telemetry pipeline to recovery plane (WORM storage)
- Inventory all non-human identity credentials and expiry timelines
- Tabletop exercises and live break-glass drills -- monthly

NEXT

6-18 months

- Deploy a secondary IdP for critical apps (Backup or Split pattern)
- App-layer token caching and graceful degradation for Tier 0 apps
- Begin issuing Verifiable Credentials alongside traditional tokens
- SPIFFE/SPIRE for workload identity across multi-cloud environments
- Evaluate OpenID Federation 1.1 for dynamic trust resolution

FUTURE

18-36 months

- Critical apps accept VCs as fallback authentication
- RFC 8693-based token exchange for cross-provider failover
- Organizational wallets for enterprise-issued VCs
- Identity chaos engineering practiced regularly
- Engage IETF / OpenID Foundation / W3C on continuity specs

Monday morning: map Tier 0 dependencies . pick one severe-but-plausible scenario . define one continuity KPI . schedule one drill

Hub-and-spoke: IRIP as the authoritative hub

The IRIP maintains authoritative identity state and serves as the coordination point for cross-environment failover.

Identity silos

Different IdPs, directories, and protocols per environment create fragmented identity state

Sync lag / split-brain

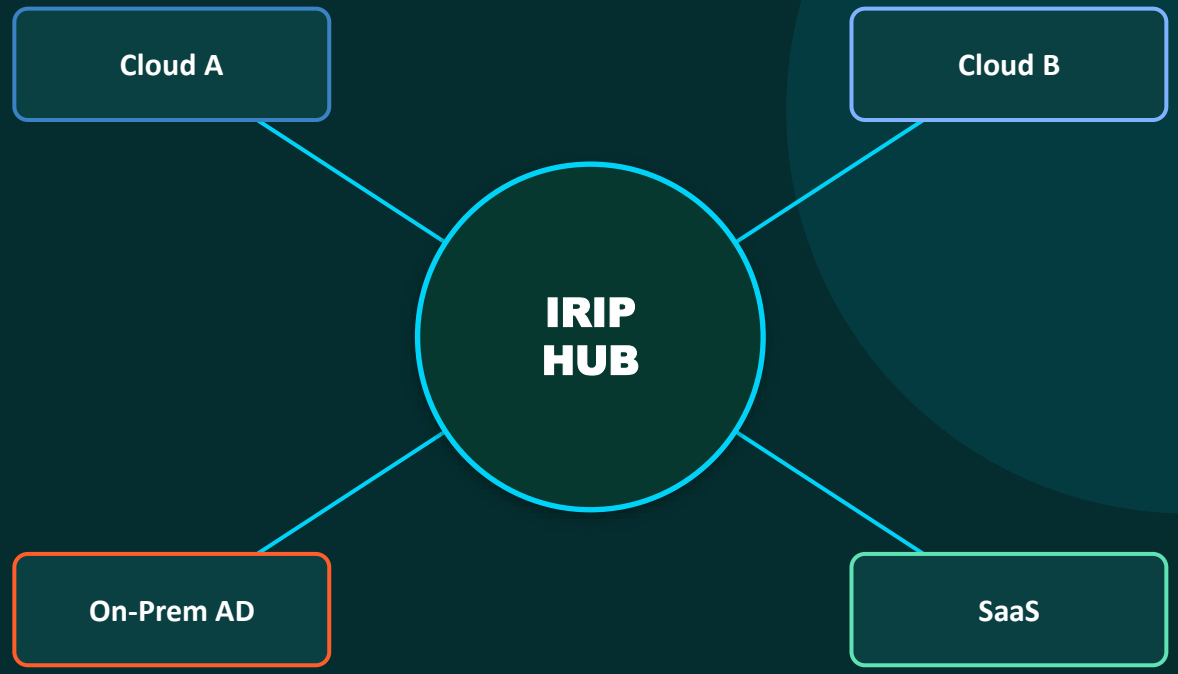
Password works on-prem but not cloud -- persists undetected for hours, compounds during incidents

Policy divergence

Conditional access behaves differently per environment -- unexpected access grants or denials during failover

NHI sprawl

Service accounts and API keys proliferating across clouds with no unified inventory or lifecycle management



One-way telemetry into hub . spokes maintain local caches + federation endpoints

Identity resilience KPI reference

These measure enterprise continuity of trusted access -- distinct from provider availability SLAs.

KPI	Measures	Target / Direction
Identity Availability	% uptime for identity services	? 99.99% for Tier 0
MTIDR	Mean time from detection to full restoration	Track vs. RTO; improve quarterly
Auth Success (Degraded)	% successful auth during disruption windows	? 95% in planned failover
Break-glass Readiness	Pass/fail: validity, scope, logging, exercise	100% readiness for recovery cohort
NHI Inventory Coverage	% NHIs with owner, purpose, privilege, lifecycle	Trend to near-complete for critical envs
Short-lived Credential Coverage	% workload/agent auth using auto-rotated creds	Increase over time; critical envs first
Exercise Pass Rate	% planned exercises meeting continuity objectives	Improve quarterly with remediation tracked
Dependency Concentration Index	% critical journeys on a single control plane	Reduce over time for top journeys

What identity providers need to rethink

Four limiting assumptions in current provider models -- and six capabilities needed over the next decade.

Reachable when needed

Unsafe under cloud concentration or tenant compromise.

Available = resilient

A service can be up yet operationally unusable.

Human IAM is separate

Business processes span workforce, workload, and agent identities simultaneously.

Shared responsibility is clear

Enterprises can't export state, don't know RPO, can't exercise restore.

- Verifiable continuity tiers -- publish RTO/RPO, restore semantics, key continuity guarantees in contract language
- Exportable, dependency-aware identity-state backup -- preserve policies, trust relationships, privileged roles, cryptographic material
- First-class degraded-mode access for pre-defined critical journeys, with explicit limits, logging, and revalidation
- Cryptographic trust anchor portability and post-quantum readiness -- lifecycle controls and continuity guarantees for keys and certs
- Native resilience evidence APIs -- backup freshness, restore rehearsal outcomes, NHI inventory completeness, credential rotation posture
- Unified governance across workforce, workload, and agent identities -- ownership, attestation, lifecycle, risk scoring, emergency containment

What changes by 2036

Six trajectories grounded in current regulatory, technical, and AI-driven trends.

Identity resilience becomes board-visible

DORA, NIS2, APRA, HKMA, and SEC all point the same direction: cyber dependency governance moves into board oversight. Identity will be reported like a critical business service.

Concentration risk harder to ignore

As enterprises consolidate into a few major control planes, regulators demand evidence that concentration is understood, governed, and mitigated.

Non-human identity is the dominant scale problem

CSA data shows governance already lagging. Over the next decade, the identity attack surface is defined by ephemeral, semi-autonomous identities.

AI policy forces better identity accountability

NIST AI RMF and EU AI Act require traceable, bounded action under authority. Identity becomes the proof mechanism for who acted, with what permissions, under whose authority.

Cryptographic agility becomes a resilience property

Post-quantum migration, passkey adoption, hardware authenticators -- continuity planning must include cryptographic dependency mapping and migration safety.

Recovery testing shifts: 'Can we trust the restore?'

From backup validation to trust validation -- can privileged boundaries be restored? Federation re-established safely? Policy state proven to match intent?