Authentic Web

Enterprise Domain Management for the New TLD Era

Proving Digital Identity Control

2026 Board Mandates for Executive Teams

What Executive Teams will be Expected to Demonstrate to Boards before AI Deployments, Regulation, and Outages Force the Issue.

"The Domain Name System (DNS) underpins every digital service. Yet DNS audits reveal compliance gaps in security policy enforcement. A brand's digital identity is the new permitter and a Brand Top-Level Domain signals trust, operating under a single end-to-end DNS security automation control environment that delivers on these board mandates."

Peter LaMantia, CEO, Authentic Web Inc.

This paper examines public statements from senior enterprise executives and boards who have declared their information security and infrastructure mandates for 2026.

It explores a ripe opportunity for executives to deliver a compelling win and deliver on board mandates, focusing on a perennially underserved enterprise weak spot: Digital Identity Management and Security of Domains and DNS Networks.

Contents

A. Executive Overview

B. Board Mandates: Implications for Executive Leadership and Teams

1. Operationalizing AI Security & Governance
2. Zero-Trust and Identity Sovereignty
3. Mandatory Regulatory Compliance
4. Cyber Resilience as "Enterprise Survival + Sovereignty"

C. Executive Playbook to Deliver 2026 Board Mandates

→ Board Mandates
× Common Failures
✓ Actions to Meet Board Mandates

D. Summary and Conclusion

A Executive Overview

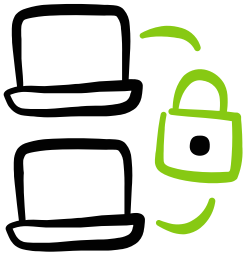
Board Expectations are Getting Real

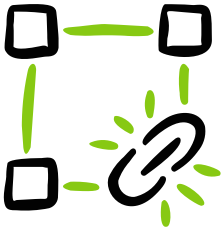
Boards no longer accept general assurances that digital identity and network risk is being managed. They require executive leadership to **prove control** over the systems that define how customers, employees, partners, and automated systems reach the business and decide what to trust.

TRUST in a brand's digital identity is the key.

Artificial Intelligence is moving out of pilots and into deployed systems that touch customer experience and operations, complete with automated identity decision-making. When those systems fail, boards focus on ownership and accountability, not technical details or nuance.

Regulatory expectations are tightening. Reporting timelines are shorter. Outages that once stayed inside IT are now communicated on the wider digital identity public spaces. These events are no longer treated as bad luck, or stuff happens but as **failures in governance oversight.**





Organizations have built sophisticated technology stacks on weakly governed digital identity foundations. External end points are fragmented across business units, teams and vendors, often without change controls. They rarely include centralized visibility nor are governed as the critical **brand identity control layer** they've become.

Why Board Mandates Have Evolved in 2026

Boards are not suddenly interested in critical infrastructure details. They are reacting to evidence and outcomes that put the business at risk, and they want more than platitudes. **They demand proof.**

Organizations are moving faster than their control systems:

→ Cloud adoption accelerated
→ SaaS usage expanded
→ Security tooling multiplied
→ AI initiatives are advancing
→ Digital Identity is trust and it is both private and public

Control was simply assumed as modernization and innovation speed took priority.

That assumption has started to break down:

→ AI is being embedded in live workflows and networks
→ Regulators expect faster and clearer explanations as well as proof of control
→ Outages caused by errors or external supply chain dependencies are now public
→ Nefarious actors are becoming more sophisticated and active, targeting the weak

Dependencies on hidden system risks has become systemic. This covers all of:

→ Supply-chain security
→ Digital identity sovereignty
→ Zero-trust architectures
→ Control plane ownership (domains, DNS, certificates)
→ AI chain of trust and authenticity

The core question has changed. Boards no longer ask if **systems are secure.** They're asking leadership to prove control, accountability, and recovery before and after something breaks.

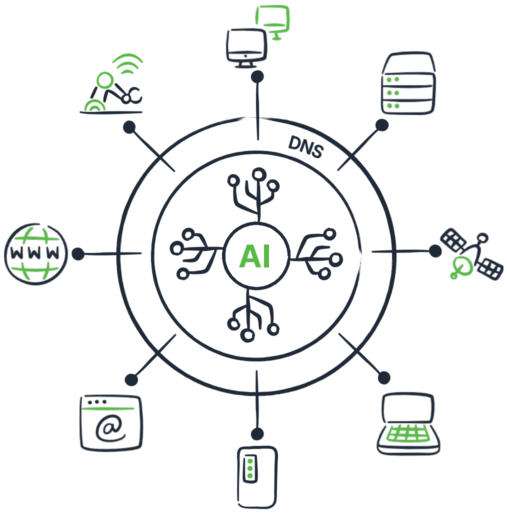
This paper outlines **Four Board Mandates** declared by medium and large organizations for 2026. It provides a playbook of direct-action that leadership can take to establish digital identity controls. With these actions leadership can deliver on the mandates, secure the business, and protect customers to GET THE WIN!

B Board Mandates: Implications for Executive Leadership & Teams

MANDATE #1
Operationalize AI Security & Governance

Why?

AI Is Now a Business Risk — Not a Science Project



AI is no longer experimental. It impacts customer experience, operational decisions, and automated workloads on proprietary networks. Boards now evaluate whether AI-driven outcomes are **predictable, defensible, and aligned.** Where accountability and control are unclear, AI shifts from a source of advantage to a source of unmanaged risk. This is the new **AIOps** which includes various requirements around observation, anomaly detection and remediation. It's all based on a foundation of digital identity trust.

Guidance for Executive Leadership

Executive leadership must ensure that AI-dependent systems resolve, connect, and exchange data only with intended and governed destinations, with clear ownership, auditable change control, and protection against silent redirection or poisoning.

Boards are increasingly inclined to make 2026 the year of "AI Return on Investment" also expressed as "AI-at-Scale" or "Make AI workloads production-grade." AI security and governance has become a conjoined critical mandate requiring CISOs to secure autonomous AI agent networks against "data poisoning" and "prompt injection" all while boards require clearer performance metrics for AI investments.

Technical Background for Operating Teams

The DNS underpins all brand digital identities, including those used by autonomous and AI-assisted systems. AI agents rely on name resolution to locate data sources, invoke services, and interact with external systems that shape their behavior.

Securing AI agents against data poisoning and prompt manipulation requires cryptographically authenticated infrastructure controls.

Enterprise-grade DNS governance prevents attackers from exploiting weak resolution paths, poisoned zones, or misconfigured records to redirect agents, manipulate upstream data sources, or inject malicious content into AI workflows and networks.

DNS auditability provides immutable records of configuration changes, limiting opportunities to hijack agent-oriented endpoints or introduce poisoned inputs.

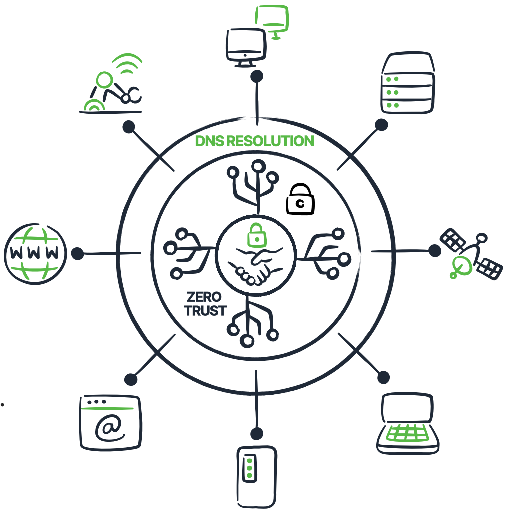
AIOps requires deterministic, trusted infrastructure inputs. DNS, without full change control, breaks that assumption. DNS change control is not optional and its governance is a foundational trust requirement.

Takeaways for Executive Leadership and Operating Teams

1. **AI security depends on control of the digital identity and routing layers AI systems inherit.** Without authoritative governance of AI-dependent identities, automated systems can behave correctly while being silently misdirected.
2. **The foundational control layer is DNS trust.** If leadership cannot prove ownership, auditability, and change control over DNS, AIOps practices and risk cannot be effectively governed at scale.

MANDATE #2
Zero Trust and Identity Sovereignty

Why?
Identity Has Replaced the Network as the New Perimeter



Identity now determines access. If identity signals are incorrect, Zero Trust controls enforce policy in the wrong place. Zero Trust has been around for 15+ years, but now it's about identity sovereignty.

Boards therefore focus on whether leadership can confidently assert who and what the organization is trusting at any given moment. Identity sovereignty becomes a governance issue when that trust is inherited implicitly rather than governed deliberately.

Guidance for Executive Leadership

Domain and DNS identity integrity, centralized control authority, security monitoring, change control auditability, and supply chain risk mitigation are required to ensure Zero Trust and identity control.

Technical Background for Operating Teams

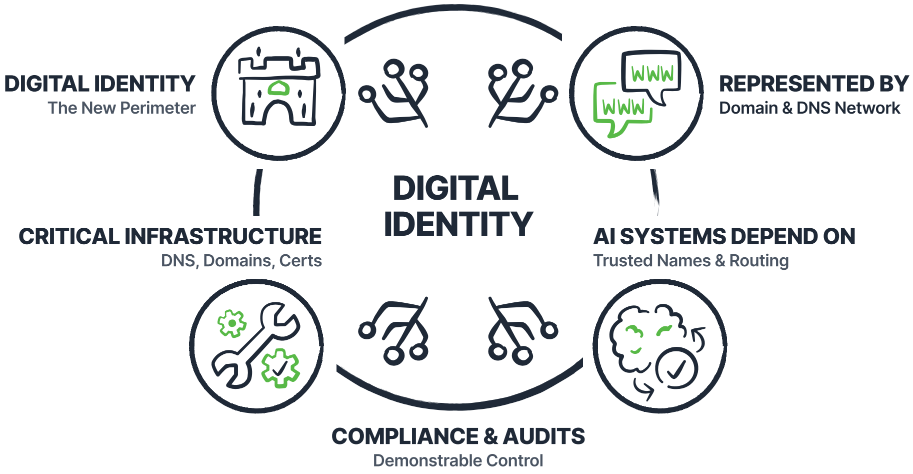
Identity sovereignty determines who controls the sources of trust an organization relies on; Zero Trust determines how access decisions are enforced against those sources.

Zero Trust architecture, where digital identity in the cloud replaces the network as the perimeter, requires hardened, auditable DNS controls. DNS is the first system that translates identity into reachability. If DNS is compromised or unaudited, identity spoofing, service impersonation, and policy bypass can occur before Zero Trust controls are evaluated.

DNS security and change auditability ensure that identity-based access decisions are enforced only against authentic, immutable service destinations. Because every identity-based request begins with name resolution, DNS sits upstream of all Zero Trust enforcement and must be treated as a vital control layer.

Takeaways for Executive Leadership and Operating Teams

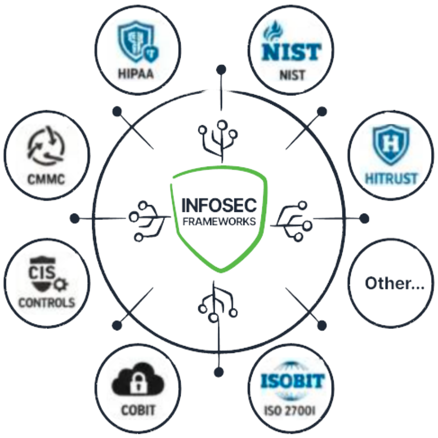
1. **Zero Trust fails if identity signals point to the wrong destination.** Without authoritative control over identity and DNS resolution, policy enforcement can occur against inauthentic services without detection.
2. **Identity sovereignty is a prerequisite, not a feature, of Zero Trust.** Leadership must govern the identities of trust the organization relies on, not simply the policies applied at the destinations, but the identity connection to the destination.



MANDATE #3
Mandatory Regulatory Compliance

Why?
Cyber Incidents Are Now Disclosure and Liability Events

Boards require rapid explanation and proof of governance. Incidents now trigger regulatory reporting, legal scrutiny, insurance review, and reputational impact in parallel, often within compressed timelines. Leadership is judged not only on what happened, but on whether controls, decision-making, and accountability can be demonstrated clearly and credibly under external examination.



Guidance for Executive Leadership

Organizations must ensure immutable audit trails, clear ownership, and evidence-ready controls for prompt and certain disclosures.

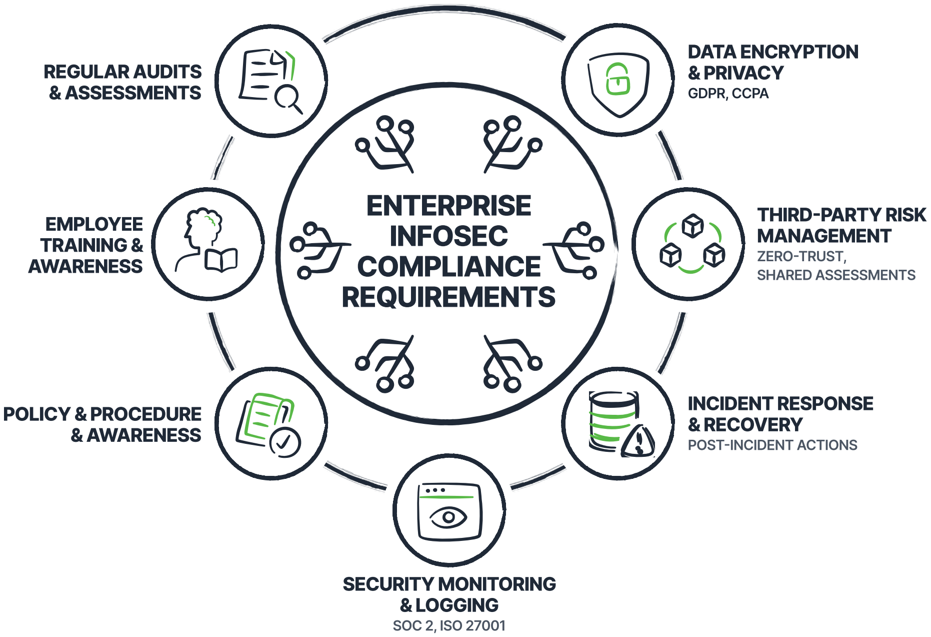
Technical Background for Operating Teams

Significant global regulations will come into force in 2026, including the EU AI Act and CIRCIA, introducing mandatory cyber-incident reporting within 72 hours and ransom payment reporting within 24 hours. These requirements shift security operations toward evidence-ready compliance, where organizations must reconstruct events, decisions, and control states under compressed timelines.

Operational teams face growing pressure to consolidate security tooling to improve visibility, change control, and auditability. At the same time, risk is increasing across "invisible" supply chains created by SaaS dependencies and third-party AI agents. These conditions demand authoritative inventories, immutable configuration records, and controls that support rapid, regulator-grade disclosure without reliance on manual reconstruction.

Takeaways for Executive Leadership and Operating Teams

1. **Regulatory compliance depends on demonstrable control, not stated intent.** Critical enterprise networks must be governed, auditable, and continuously monitored to meet modern infosec and disclosure requirements.
2. **Tool sprawl and unmanaged supply chains undermine compliance at scale.**Without consolidated, enterprise-grade control over domains and DNS, change visibility, auditability, and security assurance breaks down.


ENTERPRISE INFOSEC COMPLIANCE REQUIREMENTS
REGULAR AUDITS & ASSESSMENTS
DATA ENCRYPTION & PRIVACY
GDPR, CCPA
EMPLOYEE TRAINING & AWARENESS
THIRD-PARTY RISK MANAGEMENT
ZERO-TRUST, SHARED ASSESSMENTS
POLICY & PROCEDURE & AWARENESS
INCIDENT RESPONSE & RECOVERY
POST-INCIDENT ACTIONS
SECURITY MONITORING & LOGGING
SOC 2, ISO 27001

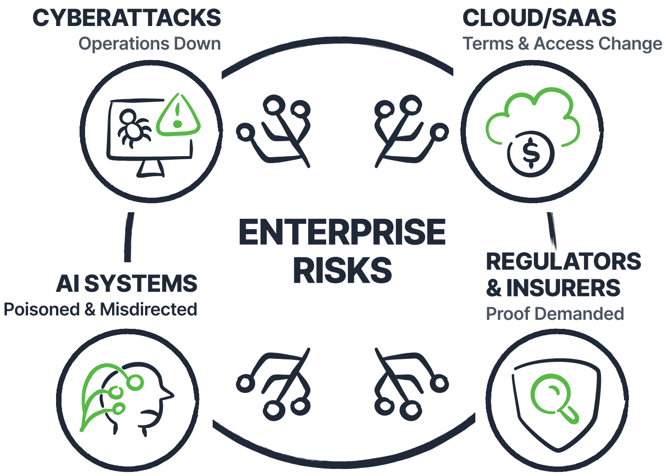
MANDATE #4

Cyber Resilience as “Enterprise Survival and Response”

Why?

Resilience Means Keeping the Business Running — Under Stress

Boards assume disruption will occur. They judge leadership by whether the organization can continue operating, communicating, and meeting obligations when controls are degraded and decisions must be made quickly. In those moments, resilience becomes a test of governance, not technology.



Guidance for Executive Leadership

Clear authority, documented recovery paths, and control over digital identity foundations are required to survive disruption.

Technical Background for Operating Teams

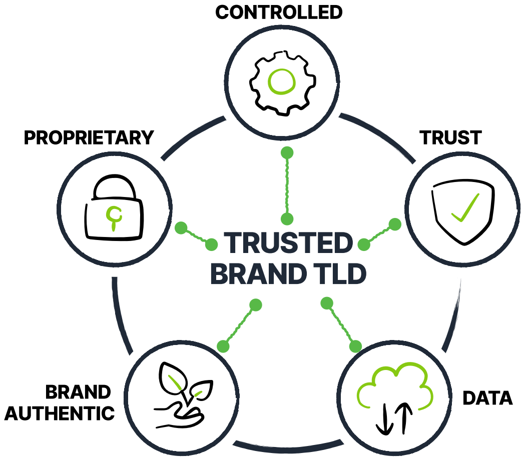
Enterprise resilience in 2026 depends on control of digital identity foundations. Domains, DNS, and certificates are no longer peripheral infrastructure; they define reachability, trust, and continuity for core business operations, including AI workloads.

Operational teams must plan for failure modes that extend beyond traditional cyberattacks, including SaaS dependency outages, misconfiguration-driven disruptions, third-party AI risk, and regulatory or insurance scrutiny requiring rapid proof of control. Resilience means the organization can continue operating during an outage or attack, trace and explain configuration changes, and restore trusted access quickly when something breaks.

This requires authoritative ownership of identity assets, auditable change control, and recovery paths that do not depend on single vendors or manual reconstruction under pressure.

Takeaways for Executive Leadership and Operating Teams

1. **Enterprise survival and digital sovereignty depend on owning what defines who you are online.** Without authoritative control over domains, DNS, and identity infrastructure, outages, vendors, or attackers can take critical operations offline.
2. **2026 offers a decision window about identity control at the root.** ICANN’s Brand TLD application window opening in April 2026 offers a path to end-to-end control of digital identity and trust, reducing third-party dependency at the most critical entry points.



C Executive Playbook to Deliver 2026 Board Mandates

Executive leadership that delivers on board mandates can start by recognizing a shift in their thinking about cybersecurity. It's no longer a generic question: **"Are we secure?"** It's **"Prove we have control, resiliency, and accountability."**

Accordingly, **PROOF** looks good to Boards in 2026. Examples are:

Capability	Board Ready Evidence from Executives
Cyber Resilience	Recovery time objectives tested & reported
AI Governance	Policy-driven controls and auditability
Compliance	Mapped controls to frameworks & disclosure rules
Digital Asset Control	Centralized with change controls and security monitoring
Risk Oversight	Regular, compliance board reporting

On Digital Identity, CISOs and their network partners must be able to answer these questions:

Board Question	Why It Matters
Who controls our domains and DNS globally?	Digital Identity Trust & Resilience
How many vendors can take us offline?	Supply Chain and Operational Risk
Can we prove change controls and oversight?	Disclosure and Compliance Risk
How would a DNS outage impact customers?	Revenue and Brand Damage Risk
Can we prove to auditors real evidence of control?	Regulatory and Insurance Readiness

THE PLAYBOOK

With proof of control, resilience, and accountability in mind, here's a playbook executive teams can follow to deliver the key assurances that the enterprise is addressing 2026 Board Mandates.

Taken together, these actions form a strategy that shifts the board's focus from identifying gaps to recognizing executive initiatives that meet the moment and position the business for long-term success.

1. Operationalize Artificial Intelligence with Security & Governance

Board Mandates

→ AI workloads must be reliable, secure, and recoverable
→ Data integrity and access control are prerequisites
→ Digital Identity trust must be assured

Common Failures

× AI pipelines depend on DNS infrastructure that is fragmented and weakly governed
× Outages are often caused by simple DNS human errors
× Identity cannot be guaranteed without control systems

Actions to Meet Board Mandates

✓ Conduct a DNS security health test to evaluate your current foundation for AI-driven services
✓ Establish proactive controls to defend against DNS-based outages and hijacks

2. Establish Digital Identity Trust and Control

Board Mandates Requirements

→ Domains, DNS, and certificates define the enterprise's digital identity
→ Loss of control = loss of trust and availability

Common Failures

× Hundreds or thousands of domains and DNS records that are ungoverned
× Multiple registrars and DNS providers make change control policies impossible
× No authoritative domain and DNS zone file inventory

Action to Meet Board Mandates

✓ Create and evaluate the business case for acquiring your own Brand Top-Level-Domain
✓ Obtain a domain & DNS security assessment to establish DNS security and management gap
  - Single vs multiple domain registrars & DNS service provider supply chain and control risk
  - DNS vulnerability visibility; orphaned IPs, dangling CNAMES, Insecure redirects, Lame delegations, SPF and DMARC coverage.

3. Establish Regulatory Governance & Disclosure Readiness

Board Mandate Requirements

→ Cyber incidents = disclosure risk
→ Governance must be provable, not implied

Common Failures

× No auditable ownership of DNS and domains
× No evidence trails for “who changed what, when, and why”
× No centralized controls to enforce DNS security policies

Action to Meet Board Mandates

✓ Demonstrate internal DNS audit history and change controls
✓ Review evidence-ready controls to support SOC 2, ISO, NIST, CIS and other framework audit or post-incident disclosure requirements

4. Establish Cyber Resilience by Design

Board Mandates

→ Minimize known risk but assume disruption
→ Demonstrate fast recovery and reporting
→ Prove resilience and readiness

Common Failure

× DNS misconfiguration, registrar and DNS provider sprawl
× No centralized control systems: Ungoverned - not monitored
× No recovery playbook for external digital dependencies

Action to Meet Board Mandates

✓ Demonstrate centralized, redundant DNS and domain controls
✓ Prove by test cases: change approval, history, rollback, and visibility
✓ Show external attack-surface resilience and monitoring

D Summary and Conclusion

Taken together, these four, surveyed, 2026 Board Mandates for cybersecurity and identity management define a new baseline for executive accountability and operational controls. From the board's view, these are not technology initiatives, and they are not security programs. They are governance expectations that boards are applying across AI, risk, compliance, and resilience.

For leadership teams, the work ahead is not to necessarily adopt more tools, but to examine whether the digital identity foundations their organizations rely on are owned, governed, and defensible. Where they are not, the risk is no longer abstract – it is structural. Only then can leaders make technology and decisions to meet the board mandate requirements. Summed up: "PROVE IT."

A board-worthy governance decision executive leaders must consider is the 2026 Brand Top-Level Domain initiative.

- ↑ Consumer Trust
- ↑ Security & Compliance
- ↓ Total Cost of Ownership
- Differentiation
- ↑ Topline Revenue
- ↑ Contribution Margin

Brand TLD Return on Investment (ROI)

A Brand TLD offers the most robust DNS security posture possible that delivers ROI

- ✓ Improve digital engagement, driving top line and margin
- ✓ Cull bloated portfolios and simplify brand protection
- ✓ Reduce long-term total cost of ownership
- ✓ Streamline change management and governance
- ✓ Automate DNS security and zone management

To learn more about Brand Top Level Domains Click Here

The implication of these mandates is that boards are increasingly asking where ultimate control of digital identity resides, and how control and resilience are demonstrated. This scrutiny has increased attention on a game-changing opportunity in trusted brand digital identity: ownership of a **Brand Top-Level Domain (TLD). Brand TLDs** represent a shift from rented, third-party dependence toward durable ownership and control of an organization's authentic digital identity. **Organizations that address these mandates deliberately will be well-positioned to engage boards, regulators, and stakeholders with confidence. Those that don't may be asked to explain why.**

If this framework is relevant to your organization, we'd be pleased to discuss how the 2026 Board Mandates apply to your digital identity control environment.

authenticweb.com

info@authenticweb.com | NA: 1-855-436-8853 | INT: +1-416-583-3770