

EXECUTIVE GUIDE

The Identity-Led Ransomware Defence Guide for Indian Enterprises

Reducing Active Directory and Kerberos blast radius before encryption begins

Introducing Time-To-Domain-Dominance (TTDD) - the governance metric that measures your real ransomware risk

Table of Contents

<u>Executive Summary</u>	5
The Strategic Risk for Indian Enterprises	5
Four Questions for the Board	5
Rapid Identity Resilience Assessment	6
<u>1. Executive Foreword</u>	7
• A Message To Business Leaders	7
• What This Guide Is For	7
• How To Use This Guide	8
<u>2. The Identity Blast Radius Model</u>	9
• Ransomware As A Control Sequence	9
• Defining Identity Blast Radius	10
• Attack Path Graph Modelling	10
• Introducing Time-To-Domain-Dominance (TTDD)	11
• Identity Risk Thresholds	11
• Board-Level Implications	12
<u>3. Understanding Active Directory As The Control Plane</u>	12
• Active Directory As Enterprise Identity Infrastructure	12
• Privilege Inheritance And Escalation Density	13
• Delegation Abuse And Structural Weakness	13
• Domain Controller Exposure Index	14
• Hybrid Identity Amplification	14
• Quantitative Control-Plane Scorecard	15
<u>4. Kerberos As The Trust Fabric</u>	16
• Kerberos In The Enterprise Authentication Lifecycle	16
• Kerberoasting As A Structural Weakness	16
• Golden Ticket Persistence Risk	17
• Silver Ticket And Service-Level Abuse	18
• Kerberos Anomaly Detection Metrics	18
• Kerberos Control Maturity Model	19

<u>5. Domain Controller Hardening And Isolation</u>	19
• Domain Controllers As The Identity Control Boundary	19
• Administrative Tier Segmentation Model	20
• Domain Controller Exposure Index (Refined Model)	20
• Replication And Trust Boundary Risk	21
• Backup And Recovery Trust Separation	21
• Manufacturing And Multi-Site Considerations	22
<u>6. Manufacturing And Multi-Site Enterprise Overlay</u>	22
• Identity In IT–OT Converged Environments	22
• OT-IT Identity Adjacency Model	24
• Vendor And Maintenance Identity Risk Index (VIRI)	24
• Operational Disruption Probability Model	25
• Multi-Site Identity Segmentation Strategy	25
• Executive Manufacturing Risk Summary	26
<u>7. Regulatory And Governance Implications In India</u>	26
• Identity Compromise As A Reporting Trigger	26
• Incident Scope Inflation Model	28
• Governance Risk Amplification	28
• Board-Level Identity Risk Dashboard	29
• From Compliance To Control	30
<u>8. The 90-Day Identity Hardening Blueprint</u>	30
• Phase 1: Days 1–30 — Exposure Quantification	30
• Phase 2: Days 31–60 — Structural Risk Reduction	31
• Phase 3: Days 61–90 — Simulation And Validation	32
• Role And Ownership Matrix	33
• TTDD Tracking Model	33
<u>9. Executive Diagnostic: Is Your Identity Estate Ransomware-Resilient?</u>	34
• Escalation Density Assessment	34
• Kerberos Governance Assessment	35
• Domain Controller Exposure Assessment	35
• Manufacturing And Multi-Site Overlay	36
• TTDD Executive Indicator	36
• Diagnostic Summary Scoring	37

<u>10. Operating Model For Continuous Identity Risk Reduction</u>	37
• Quarterly Identity Risk Review Cadence	38
• Change-Driven Risk Reassessment	38
• Continuous Simulation Model	39
• Identity Telemetry Integration	39
• Executive Accountability Structure	40
<u>11. From Framework To Execution: Governance Imperatives</u>	40
<u>12. Conclusion: Identity Defence As A Governance Imperative</u>	41
<u>Appendix</u>	43
• Key Definitions	43
• Attack Technique Reference	43
• Metric Reporting Template	44

Executive Summary

Most ransomware events that escalate to enterprise-wide disruption do not begin with a failure of detection. They begin with a failure of identity control. When an attacker can traverse privilege pathways from a single compromised account to domain-level authority in a matter of hours, the scope of damage is determined before encryption begins.

This guide introduces a measurable framework for understanding and reducing that risk. Its central metric is Time-To-Domain-Dominance (TTDD): the estimated elapsed time between initial compromise and an attacker achieving domain-level control. In poorly governed identity estates, TTDD can be measured in hours. In hardened environments, it can be extended beyond a full detection and response cycle - giving defenders the window they need to contain the threat.

The Strategic Risk For Indian Enterprises

Indian enterprises face a compounded version of this challenge. Multi-site manufacturing operations, IT/OT convergence, distributed plant authentication, and complex vendor access arrangements create privilege relationships that expand attack surface well beyond corporate IT boundaries. A ransomware event that achieves domain dominance in a corporate forest can propagate to plant systems, triggering not just data loss but production stoppage. In regulated sectors - financial services, telecom, critical infrastructure - the same event can trigger mandatory reporting obligations under CERT-In directions and the Digital Personal Data Protection Act within hours of discovery.

Four Questions For The Board

This guide is organised to help boards and senior leadership teams answer four questions that recovery planning alone cannot address:

- How quickly could an attacker with a single compromised account reach domain-level control in our environment?
- Does a ransomware event in our corporate domain put our plant and operational systems at risk?
- Are our regulatory reporting obligations understood and can they be met within mandatory timeframes if an identity incident occurs?
- What would a 90-day programme to materially reduce our identity exposure cost, and what would it change?

If you cannot answer these questions with data, this guide provides the framework to do so. The technical detail that follows supports a non-technical conclusion: identity governance is a board-level risk control, and it can be measured, engineered, and improved.

Rapid Identity Resilience Assessment

Before reading further, consider the following five questions. If your security leadership cannot answer any of them with data — not policy documentation, but measured data — this guide addresses the gap directly. A full diagnostic is provided in Section 9.

Question	Yes	No	Unknown
What is our current Time-To-Domain-Dominance?	☐	☐	☐
How many privilege escalation paths exist from a standard user account to Domain Admin?	☐	☐	☐
Has our KRBTGT account been dual-rotated and validated in the last 12 months?	☐	☐	☐
Are our domain controllers isolated from general-purpose user and server networks?	☐	☐	☐
If ransomware encrypted our corporate domain tonight, which plant or operational systems would be unreachable by morning?	☐	☐	☐

Two or more Unknown responses indicate that identity risk is not currently measurable at the governance level. This guide provides the framework to change that.

1. Executive Foreword

A Message To Business Leaders

The ransomware question boards are asking - are our backups immutable, is our response plan tested, have we purchased the right insurance - is the wrong question. Recovery capability matters. But the outcome of a ransomware event is largely determined before encryption begins, by decisions about identity governance that were made months or years earlier.

In the incidents that produce the largest losses - those measured in weeks of recovery time, in regulatory investigations, in operational shutdowns - attackers did not overwhelm defences. They walked a path of least resistance through an identity estate that gave them too much access, too quickly. By the time encryption was deployed, they had been in control of the environment for hours.

The question your security team should be answering - and that the board should be asking - is not whether backups work. It is how long it would take an attacker, starting from a single compromised employee account, to reach the systems that control your entire organisation. In many enterprises, the answer is measured in hours. That is the risk this guide is designed to address.

For Indian enterprises, this challenge is sharper than it may appear. Complex multi-site structures, manufacturing environments where IT and operational technology intersect, and a growing regulatory reporting burden under CERT-In and the DPDP Act mean that an identity failure does not stay contained to IT. It propagates to operations, to regulators, and to the boardroom.

What This Guide Is For

This guide is written for business leaders who need to understand identity risk in terms that support governance decisions, not for those who manage the technical controls day to day. It introduces a measurable concept - Time-To-Domain-Dominance - that allows executives to track identity resilience with the same discipline applied to financial or operational risk. It provides a diagnostic that leadership teams can use to assess their current exposure. And it sets out a 90-day blueprint that converts assessment into structured risk reduction.

Security teams have the technical depth to implement the controls described here. The role of senior leadership is to ensure those teams have governance mandate, resource prioritisation, and board-level accountability structures that make implementation possible and sustained.

Identity control is not an IT hygiene matter. It is a structural risk variable that determines whether a ransomware event becomes a contained incident or a board-level crisis. The organisations that experience the worst outcomes are rarely those with the weakest perimeter defences. They are those where the path from a single compromised account to organisation-wide control was too short, and where nobody had measured it.

How To Use This Guide

The guide moves from risk model to technical control to governance structure. Sections 2 through 5 build the analytical foundation - explaining how blast radius is calculated, how Kerberos governs identity trust, and how domain controller exposure is measured. Sections 6 and 7 apply this to the specific conditions of Indian enterprise environments: multi-site manufacturing, IT/OT convergence, and the regulatory obligations that identity failures can trigger. Sections 8 through 11 are operational - a 90-day hardening blueprint, a diagnostic, a continuous governance model, and an execution framework. Readers who need to reach a decision quickly should start with the Rapid Identity Resilience Assessment and the diagnostic in Section 9; those responsible for programme delivery should treat Section 8 as the primary reference.

2. The Identity Blast Radius Model

Ransomware As A Control Sequence

Enterprise Vignette: Multi-Site Manufacturing Group, Western India

A large diversified manufacturing group operating across three Indian states experienced a credential phishing incident affecting a mid-level IT administrator. Within four hours, attackers traversed nested group memberships, leveraged a poorly governed service account, and reached domain-level authority in the corporate forest.

Encryption was deployed later that night. The operational disruption did not begin with malware execution. It began when identity control shifted.

Post-incident analysis showed over 120 privilege escalation paths to Tier 0, unconstrained delegation in two domains, and no recent KRBTGT validation.

Recovery took three weeks. Production loss was measured in days. The decisive failure was structural, not reactive.

Ransomware impact follows a structured control sequence, not a random outbreak pattern. The sequence typically progresses as follows:

Initial Access
→ Privilege Escalation
→ Domain Dominance
→ Policy Control
→ Encryption And Data Exfiltration

Encryption is the visible stage. Domain dominance is the decisive stage. Once an attacker can modify Group Policy, create privileged accounts, disable security tooling, or access backup credentials, ransomware deployment is operationally straightforward. Containment becomes significantly harder and the scope of recovery expands to match whatever the attacker was able to reach during the hours they held control.

Blast radius is determined by how far identity control propagates.

Defining Identity Blast Radius

Identity blast radius refers to the total number of systems, services, and trust relationships that become reachable once privileged identity control is achieved. Blast radius is influenced by:

- Privilege inheritance density
- Delegation configuration
- Service account sprawl
- Cross-domain trusts
- Domain controller exposure
- Hybrid identity synchronisation boundaries

In large Indian enterprises operating multi-site or multi-plant domain structures, blast radius may span corporate data centres, regional plants, vendor access environments, and cloud workloads. A flat privilege structure produces exponential blast radius growth. A tiered and segmented structure constrains propagation.

Attack Path Graph Modelling

Modern identity risk assessment treats Active Directory as a graph. Nodes represent identities, groups, service accounts, and domain controllers; edges represent permission relationships, delegation rights, and trust boundaries. Privilege escalation risk is calculated by identifying the shortest path from a low-privilege node to a high-privilege node such as Domain Admin. Key metrics include:

- Total escalation path count
- Average hop count to domain dominance
- Number of privileged service account bridges
- Cross-domain trust adjacency paths
- Kerberos-dependent escalation chains

High path density correlates with lower Time-To-Domain-Dominance. Graph-based modelling replaces assumption with evidence.

Introducing Time-To-Domain-Dominance (TTDD)

Time-To-Domain-Dominance measures the estimated time required for an attacker to achieve domain-level control starting from an initial compromise. TTDD is influenced by:

- Number and length of escalation paths
- Password strength and service account entropy
- Delegation exposure
- Domain controller accessibility
- Kerberos ticket governance
- Detection and response maturity

In baseline enterprise environments, TTDD may be measured in hours. In hardened environments with constrained privilege graphs and Kerberos governance discipline, TTDD can extend beyond a full detection and containment cycle. Extending TTDD increases defensive leverage and detection opportunity.

Identity Risk Thresholds

For executive governance, identity risk can be categorised into three maturity bands:

Risk Band	Characteristics	TTDD Estimate
High Exposure	Multiple direct paths to Domain Admin under four hops; roastable privileged service accounts; domain controllers reachable from user subnets; no recent KRBTGT rotation	< 6 hours
Moderate Exposure	Delegation partially constrained; privileged access tiering implemented but not consistently enforced; service account rationalisation underway	6 – 24 hours
Controlled Exposure	Tiered administration enforced; roastable accounts eliminated; DC isolation validated; Golden Ticket simulation tested and contained	> 24 hours

This maturity framing allows executive reporting without technical oversimplification.

Board-Level Implications

Board discussions frequently focus on recovery time objectives and backup resilience, which are legitimate concerns but incomplete ones. Identity blast radius reframes the question: not how quickly can we recover, but how large will the recovery scope be. If domain dominance is achieved quickly, the scope expands across business units, plants, and cloud environments, with regulatory exposure and forensic uncertainty widening in proportion. If TTDD is extended and privilege pathways are constrained, ransomware events are more likely to be contained before they become systemic. That is the difference identity engineering makes, and it is why the topic belongs on the governance agenda.

3. Understanding Active Directory As The Control Plane

Active Directory As Enterprise Identity Infrastructure

Active Directory is not simply a directory service. In large enterprises it functions as the identity control plane governing:

- Authentication across users, servers, and applications
- Authorisation through group membership and delegation
- Policy enforcement via Group Policy Objects
- Trust relationships across domains and forests
- Synchronisation with cloud identity platforms

When privilege escalation reaches this control plane, the attacker can influence identity decisions at scale. The impact surface extends beyond individual systems to policy propagation across business units, plants, and cloud-connected workloads.

Privilege Inheritance And Escalation Density

Privilege inheritance is cumulative. Over time, users and service accounts accumulate permissions through nested group memberships, delegated administrative rights, application-driven privilege requirements, temporary access not revoked, and cross-domain trusts. This accumulation creates escalation density.

Escalation Density Illustration

Metric	Low Risk Estate	Moderate Risk Estate	High Risk Estate
Avg Hop Count To Domain Admin	> 6	4 – 6	< 4
Privileged Service Accounts	< 20	20 – 100	> 100
Direct User → DC Paths	0	Limited	Multiple
Delegation Scope	Constrained	Partially Constrained	Unconstrained Present
TTDD Estimate	> 24 hrs	6 – 24 hrs	< 6 hrs

Lower hop count combined with high service account exposure correlates directly with reduced TTDD.

Delegation Abuse And Structural Weakness

Delegation allows accounts to act on behalf of others. When misconfigured, it becomes a structural escalation bridge. Delegation risks include unconstrained delegation, excessive resource-based constrained delegation, service accounts with write permissions to privileged groups, and cross-domain delegated rights.

Risk can be conceptualised as a matrix plotting delegation breadth (number of systems reachable) against privilege level of delegated accounts. High values on both axes indicate systemic risk. This heat-mapping approach allows enterprises to prioritise delegation reduction where blast radius impact is highest.

Domain Controller Exposure Index

Domain controller exposure can be measured through an exposure index combining access surface and privilege adjacency.

Component	Measurement Criteria	Risk Signal
Administrative Access Surface	Number of hosts allowed RDP/remote admin	High surface increases escalation probability
Credential Reuse	Shared admin credentials present	Enables lateral privilege reuse
Replication Boundaries	Cross-site replication trust scope	Expands blast radius
Backup Isolation	Backup admin within production trust	Enables recovery compromise
Monitoring Coverage	Kerberos anomaly detection active	Low coverage delays detection

A high exposure index combined with short hop counts indicates high probability of rapid domain dominance.

Hybrid Identity Amplification

When Active Directory synchronises with cloud identity platforms, the control plane extends beyond on-prem infrastructure. Hybrid amplification factors include cloud admin roles mapped to on-prem groups, federated authentication trust, conditional access misconfiguration, and service principals with broad permissions.

Compromised User
→ On-Prem Privilege Escalation
→ Synced Cloud Admin Role
→ SaaS Control
→ Data Exfiltration

Hybrid amplification increases the total reachable identity blast radius even if on-prem controls appear constrained.

Quantitative Control-Plane Scorecard

To operationalise control-plane governance, enterprises can track a structured scorecard.

Control Area	Current State	Target State	Risk Trend
Escalation Path Count	Numeric	Reduced > 60%	↓
Roastable Accounts	Numeric	< 5% Privileged	↓
Domain Controller Exposure Index	High / Medium / Low	Low	↓
Delegation Exceptions	Numeric	Eliminated	↓
TTDD	Hours	> 24 hrs	↑

Quarterly tracking of these indicators shifts identity from a configuration management activity to a risk engineering discipline. Active Directory is a measurable control plane, and without quantitative visibility it will always be governed reactively.

4. Kerberos As The Trust Fabric

Kerberos In The Enterprise Authentication Lifecycle

Kerberos governs how identities prove themselves within Active Directory. It issues time-bound tickets that grant access to services without repeatedly transmitting credentials. The simplified lifecycle is as follows:

- User authenticates and receives a Ticket Granting Ticket (TGT).
- TGT is used to request service tickets (TGS) for specific resources.
- Service tickets grant access to applications, servers, and privileged services.

If the integrity of TGT or TGS issuance is compromised, identity assurance collapses.

User Credential
→ TGT Issuance
→ TGS Request
→ Service Access
→ Policy Enforcement

Control weaknesses at the TGT or delegation layer propagate across the entire authentication chain.

Kerberoasting As A Structural Weakness

Kerberoasting exploits service accounts with Service Principal Names (SPNs). Attackers request valid service tickets and attempt offline password cracking. Risk variables include password entropy of service accounts, privilege level of the service account, delegation rights associated with the account, and age of credential rotation.

Metric	Low Exposure	Moderate Exposure	High Exposure
Privileged SPN Accounts	< 5%	5 – 15%	> 15%
Password Length	> 25 chars random	16 – 25 chars	< 16 chars or static
Rotation Frequency	≤ 90 days	90 – 180 days	> 180 days
Delegation Rights	Constrained	Mixed	Unconstrained

High roastable exposure reduces TTDD because cracked credentials often bridge to privileged groups.

Golden Ticket Persistence Risk

Golden Ticket attacks rely on compromise of the KRBTGT account hash. With it, attackers can forge TGTs and impersonate any identity. Golden Ticket capability enables persistent privileged access, undetected impersonation, bypass of password resets, and long-term stealth control.

Scenario	Baseline Estate	Hardened Estate
KRBTGT Rotation Discipline	Inconsistent	Dual reset enforced
Forged TGT Validity	Accepted	Invalidated post-rotation
Domain Admin Impersonation	Successful	Blocked
TTDD	< 3 hrs	> 24 hrs
Alert Fidelity	Low	High-confidence anomaly alerts

Golden Ticket resilience must be validated through controlled simulation.

Silver Ticket And Service-Level Abuse

Silver Ticket attacks target individual services by forging service tickets without interacting with the domain controller. Risk implications include persistence at service layer, bypass of centralised monitoring, and targeted access to high-value systems. Silver Ticket risk increases when service accounts possess excessive local privileges on critical servers.

Kerberos Anomaly Detection Metrics

Kerberos governance requires behavioural detection metrics.

Indicator	Risk Signal	Governance Action
Abnormal TGT Lifetime	Possible forged ticket	Validate KRBTGT integrity
Excessive TGS Requests	Potential Kerberoasting	Audit SPN accounts
Ticket Requests From Non-Admin Hosts	Escalation attempt	Trigger investigation
Replication Anomalies	Possible DC compromise	Isolate replication path
LSASS Memory Access Events	Credential extraction attempt	Endpoint containment

Detection must correlate identity, endpoint, and network telemetry.

Kerberos Control Maturity Model

Kerberos security maturity can be categorised as follows:

Maturity Level	Characteristics
Level 1 — Reactive	Service accounts unmanaged; no KRBTGT rotation validation; minimal anomaly monitoring
Level 2 — Structured	Periodic service account review; delegation partially constrained; event log monitoring enabled
Level 3 — Controlled	Privileged service accounts minimised; dual KRBTGT rotation enforced; Kerberos anomaly detection integrated with XDR; Golden Ticket simulation validated annually

Advancing through this maturity model increases TTDD and reduces the risk of silent, long-term persistence. An estate that has reached Level 3 is one where an attacker who compromises the KRBTGT account cannot maintain forged ticket access indefinitely, and where the anomalies generated by Kerberoasting attempts are likely to be detected.

5. Domain Controller Hardening And Isolation

Domain Controllers As The Identity Control Boundary

Domain controllers enforce authentication, authorisation, replication, and policy distribution. Compromise at this layer is categorically different from compromise of a member server: it converts escalation into systemic control, giving an attacker the ability to manipulate identity decisions across the entire estate. Domain controller hardening is therefore boundary engineering, not routine system configuration. Once controllers are reachable from general-purpose networks, the structural conditions for rapid domain dominance are in place.

Administrative Tier Segmentation Model

Effective hardening begins with tiered administration.

Tier	Scope	Access Source	Key Controls
Tier 0	Domain Controllers, KRBtgt, Forest Trusts	Dedicated hardened admin workstations	No internet access, MFA enforced, no lateral reuse
Tier 1	Member Servers, Application Servers	Segmented admin hosts	Limited delegation, monitored elevation
Tier 2	User Workstations	Standard IT admin endpoints	No privileged credential caching

Cross-tier credential reuse must be eliminated. If Tier 2 credentials can access Tier 0 systems, TTDD compresses.

Domain Controller Exposure Index (Refined Model)

The Domain Controller Exposure Index (DCEI) quantifies the probability of rapid domain dominance.

Dimension	Measurement	Low Risk	High Risk
Admin Access Surface	# of systems allowed admin login to DC	< 5	> 25
Replication Trust Scope	# of domains with replication rights	Segmented	Broad, multi-site
Credential Reuse	Shared admin accounts present	None	Multiple
Backup Isolation	Backup admin outside production trust	Yes	No
Monitoring Integration	Real-time Kerberos + DC telemetry	Integrated	Siloed logs

A high DCEI score combined with short hop counts indicates elevated systemic risk.

Replication And Trust Boundary Risk

Replication ensures consistency across domain controllers. It also expands blast radius if boundaries are flat. Risk conditions include unrestricted replication between sites, legacy trusts from acquired entities, shared service accounts across forests, and lack of replication path monitoring.

Replication Scope	Isolation Level	Escalation Impact
Single-Site Only	Segmented	Localised
Multi-Site, Controlled	Partially Segmented	Regional
Multi-Forest, Unrestricted	Flat Trust	Enterprise-Wide

Replication must be evaluated as a blast-radius multiplier.

Backup And Recovery Trust Separation

Backups are ineffective if backup identities reside within the same trust boundary as production domains.

Control Area	Required State
Backup Admin Accounts	Separate credentials, no domain reuse
Storage Access	Segmented from production AD
Credential Vaulting	Hardware-backed or isolated vault
Restore Simulation	Tested without production credential dependency

If attackers can reach backup credentials after domain dominance, recovery timelines extend significantly.

Manufacturing And Multi-Site Considerations

In multi-plant or distributed manufacturing estates, domain controller hardening must account for local domain controllers supporting plant authentication, WAN-linked replication paths, vendor remote maintenance access, and legacy production systems unable to support modern hardening baselines.

Control Factor	Centralised Enterprise	Multi-Plant Enterprise
DC Count	Limited	Distributed
Replication Paths	Fewer	Numerous
Vendor Access	Controlled	Often Persistent
TTDD Risk	Moderate	Elevated Without Segmentation

Segmentation between corporate and plant identity boundaries reduces disruption risk, sometimes dramatically. Without isolation, monitoring, and segmentation, privilege escalation pathways converge toward domain dominance faster than most detection programmes can respond.

6. Manufacturing And Multi-Site Enterprise Overlay

Identity In IT–OT Converged Environments

In manufacturing enterprises, identity does not stop at corporate IT boundaries. It frequently extends into plant networks, production support systems, and OT-integrated authentication services.

Enterprise Vignette: Pharmaceutical Manufacturer, Southern India

A mid-sized pharmaceutical manufacturer operating across four production sites experienced a ransomware event that began with a compromised vendor support account. The vendor had been granted persistent access to the corporate domain to maintain an ERP integration. That account held delegated rights that had never been reviewed since the original project implementation three years earlier.

From the vendor account, attackers escalated through a service account shared between the corporate domain and the plant authentication environment. Within six hours they had reached domain-level control. Encryption was deployed across production scheduling systems and manufacturing execution systems simultaneously. Two sites lost the ability to track batch production against quality specifications, triggering a mandatory product hold across all four facilities pending audit.

The decisive failure was the trust bridge between the vendor account and the plant authentication domain. If a segmented gateway and time-bound access had been enforced, the blast radius would have been constrained to the corporate environment. Instead, operational continuity was the price of an identity governance gap that could have been closed without any capital expenditure.

Identity adjacency in manufacturing environments often includes:

- Plant-level domain controllers synchronised with corporate AD
- MES and ERP service accounts with elevated privileges
- Vendor remote maintenance identities
- Shared authentication for production monitoring systems

When privilege escalation reaches these identity bridges, operational impact becomes immediate rather than theoretical.

OT-IT Identity Adjacency Model

Compromised Corporate User
→ Privilege Escalation In Corporate AD
→ Trust Propagation To Plant Domain
→ Authentication Control Over MES / Production Systems
→ Operational Disruption Risk

The shorter the trust path between corporate identity and plant systems, the higher the operational blast radius.

Vendor And Maintenance Identity Risk Index (VIRI)

Vendor identities frequently represent persistent adjacency risk.

Dimension	Low Risk	Moderate Risk	High Risk
Access Duration	Time-bound	Extended	Persistent
Privilege Scope	Limited, least privilege	Mixed	Broad admin rights
Network Segmentation	Isolated jump host	Partial segmentation	Direct plant access
Credential Governance	MFA + rotation	MFA only	Static passwords
Monitoring	Session recorded	Partial logging	Minimal logging

High VIRI combined with high escalation density materially increases plant-level ransomware exposure.

Operational Disruption Probability Model

Identity risk in manufacturing must be evaluated against operational continuity.

Factor	Impact On Production
Plant DC Compromise	Authentication failure across production systems
MES Service Account Escalation	Manipulation of production data or stoppage
Vendor Identity Abuse	Unauthorised configuration changes
Replication Across Sites	Multi-plant outage potential

Operational disruption probability increases when TTDD is short and replication scope is broad.

Multi-Site Identity Segmentation Strategy

Effective containment requires segmentation at identity boundary layers.

Boundary	Required Control
Corporate To Plant AD	Conditional trust with monitoring
Vendor To Plant Systems	Time-bound access via hardened gateway
Backup To Production Identity	Separate credentials and vault
Cloud To On-Prem	Strict role mapping and audit

Executive Manufacturing Risk Summary

In distributed manufacturing enterprises, identity is not a back-office concern — it is an operational dependency. If privilege escalation reaches plant-level identity systems, recovery planning alone cannot prevent production impact. A ransomware event that might have been contained to corporate IT becomes a multi-site operational failure when the identity boundaries between those environments are flat. Reducing escalation density, constraining trust propagation, and isolating plant authentication boundaries are the controls that make the difference between a contained IT incident and a production shutdown.

7. Regulatory And Governance Implications In India

Identity Compromise As A Reporting Trigger

In India, identity compromise is not only a technical failure. It can become a statutory reporting event. Where privilege escalation results in unauthorised access to systems containing personal or sensitive business data, enterprises may trigger reporting obligations under three distinct frameworks.

CERT-In Incident Reporting Directions

CERT-In's 2022 directions require mandatory notification of cybersecurity incidents within six hours of detection. Ransomware is explicitly listed as a notifiable incident category. The six-hour window is operationally demanding: it requires that enterprises not only detect the incident quickly, but that they can characterise its scope accurately enough to make a credible notification. When domain dominance has been achieved and forensic integrity is uncertain, scoping becomes speculative. Enterprises that cannot confirm what systems were accessed, or what credentials were exposed, face the unenviable choice between under-reporting and over-reporting, both of which carry regulatory risk.

The connection between identity hardening and CERT-In compliance is direct. When escalation pathways are short and domain dominance is achieved rapidly, the scope of a ransomware event becomes enterprise-wide before detection occurs. Conversely, when TTDD is extended and privilege pathways are constrained, incidents are more likely to be detected while still localised - making the scope of a mandatory notification both smaller and more defensible.

Digital Personal Data Protection (DPDP) Act 2023

The Digital Personal Data Protection Act 2023 imposes obligations on data fiduciaries to implement appropriate technical and organisational measures to protect personal data, and to notify the Data Protection Board and affected individuals of personal data breaches. When domain dominance is achieved, the probability that systems containing personal data were accessed rises sharply - even if encryption was the primary objective. Enterprises that lack visibility into which systems an attacker traversed during privilege escalation cannot reliably determine whether a personal data breach occurred, leaving them legally exposed and unable to demonstrate the security measures that DPDP requires. Identity governance directly reduces this exposure by limiting the systems reachable during escalation and by preserving the audit integrity needed to reconstruct events after the fact.

Sectoral Regulations: RBI, SEBI, And Critical Infrastructure

Sector-specific obligations add a further layer of exposure. The Reserve Bank of India's cybersecurity framework for regulated entities requires banks and payment system operators to implement privileged access management controls and to report cyber incidents to RBI within defined timelines, with SEBI imposing parallel obligations on market infrastructure institutions and registered intermediaries. The Department of Telecommunications has introduced cybersecurity rules for licensed entities that include identity governance requirements. In critical infrastructure sectors designated under the Information Technology Act, a ransomware event affecting operational systems may trigger scrutiny beyond standard incident reporting. Organisations operating across these sectors should map their identity control posture against each applicable regulatory framework, not solely against the CERT-In baseline.

The scope of reporting expands when domain dominance prevents accurate containment scoping.

Incident Scope Inflation Model

When domain-level control is achieved, forensic clarity declines.

Escalation Stage	Containment Scope	Regulatory Exposure
Compromised User Only	Localised	Limited
Privileged Server Access	Departmental	Moderate
Domain Dominance	Enterprise-Wide	High
Multi-Site Replication Impact	Cross-Region	Severe

As escalation progresses, uncertainty regarding data access expands. This increases reporting scrutiny and executive accountability.

Governance Risk Amplification

Privilege escalation amplifies governance risk through loss of audit integrity, policy manipulation capability, log tampering risk, and backup compromise possibility.

Governance Domain	Identity Failure Impact
Data Protection	Inability to confirm data access boundaries
Financial Reporting	Risk to system integrity controls
Operational Continuity	Potential production stoppage
Cyber Insurance	Increased claim scrutiny and exclusions

Constraining escalation pathways narrows regulatory uncertainty.

Board-Level Identity Risk Dashboard

Executive Callout: What The Board Should See

- Current escalation path count
- TTDD baseline and quarterly trend
- Domain Controller Exposure Index band
- Golden Ticket simulation result
- Privileged service account exposure percentage

If these metrics are unavailable, identity governance is not measurable. Identity risk should be reported in measurable terms rather than tool coverage metrics.

Metric	Current Value	Target Value	Risk Direction
Escalation Path Count	Numeric	Reduced > 60%	↓
Roastable Privileged Accounts	%	< 5%	↓
Domain Controller Exposure Index	High / Medium / Low	Low	↓
TTDD	Hours	> 24 hrs	↑
Golden Ticket Simulation Result	Pass / Fail	Pass	↑

Reporting these metrics quarterly elevates identity from IT hygiene to board-level resilience tracking.

From Compliance To Control

Regulatory compliance frameworks set a floor, not a ceiling. Meeting CERT-In notification requirements, satisfying DPDP obligations, and passing RBI cyber assessments do not in themselves prevent domain dominance. An organisation can be fully compliant with every applicable framework and still have a TTDD measured in hours. The value of identity engineering lies not in its compliance contribution, though that is real, but in its preventive effect: when escalation density is reduced and TTDD is extended, the blast radius that determines regulatory exposure narrows before an incident occurs. Identity governance becomes a preventive control rather than a post-incident documentation exercise.

8. The 90-Day Identity Hardening Blueprint

90-Day Outcome Targets

- Reduce escalation paths by at least 40%
- Eliminate unconstrained delegation
- Rotate and validate KRBTGT twice
- Isolate Tier 0 administrative access
- Establish TTDD baseline and post-hardening delta

Identity risk reduction must move from assessment to execution. A structured 90-day programme reduces escalation density and extends TTDD.

Phase 1: Days 1–30 - Exposure Quantification

The first phase establishes a measurable baseline.

Phase 1 Objectives

- Conduct full attack path graph analysis
- Inventory all privileged users and service accounts
- Identify roastable SPN accounts
- Calculate Domain Controller Exposure Index (DCEI)
- Estimate baseline TTDD through controlled modelling

Deliverable	Measurement	Executive Value
Escalation Path Count	Numeric	Quantifies blast radius
Roastable Privileged Accounts	% of total	Indicates Kerberoasting risk
DCEI Score	High / Medium / Low	Control-plane exposure clarity
Baseline TTDD	Hours	Risk urgency indicator

Baseline visibility replaces assumption with data, and data is the precondition for prioritising where structural changes will have the greatest effect on TTDD.

Phase 2: Days 31–60 - Structural Risk Reduction

The second phase focuses on removing structural escalation bridges.

Priority Controls

- Remove unconstrained delegation
- Rationalise or de-privilege service accounts
- Enforce tiered administrative model
- Implement phishing-resistant MFA for privileged identities
- Isolate domain controller administrative access
- Separate backup identities from production trust

Control Action	Direct Impact On TTDD	Blast Radius Effect
Delegation Removal	Increases hop count	Reduces escalation density
Service Account Reduction	Eliminates privilege bridges	Reduces Kerberos abuse risk
Tier Enforcement	Blocks cross-tier reuse	Slows lateral movement
DC Isolation	Restricts control-plane access	Prevents rapid domain dominance

By Day 60, measurable contraction in escalation path count should be visible in the attack graph, and the DCEI score should reflect the reduction in administrative surface around domain controllers.

Phase 3: Days 61–90 - Simulation And Validation

The third phase validates control integrity.

Validation Activities

- Golden Ticket simulation under monitored conditions
- Kerberoasting attempt modelling
- Lateral movement simulation across sites
- Backup restoration exercise with isolated credentials
- TTDD recalculation under hardened state

Metric	Baseline	Post-Hardening	Risk Direction
Escalation Path Count	Numeric	Reduced	↓
Roastable Accounts	Numeric	Reduced	↓
DCEI	High / Medium / Low	Lower	↓
TTDD	Hours	Increased	↑
Golden Ticket Simulation	Successful / Blocked	Blocked	↑

Validation ensures that policy statements and configuration changes have translated into measurable resilience, not just documented intentions. A TTDD that has not improved after 90 days of remediation indicates that the structural changes made were insufficient or that new escalation paths have emerged.

Role And Ownership Matrix

Identity hardening requires cross-functional execution.

Role	Responsibility
CISO	Executive oversight and governance reporting
Identity Architect	Attack path modelling and structural redesign
Infrastructure Team	Tier implementation and DC isolation
SOC	Kerberos anomaly detection integration
OT / Plant IT	Segmentation of plant-level domains

Clear ownership prevents implementation drift, which is the most common reason identity hardening programmes stall after the initial assessment phase.

TTDD Tracking Model

Time-To-Domain-Dominance should be recalculated quarterly.

Quarter	TTDD (Hours)	Escalation Path Count	DCEI	Risk Trend
Q1	Baseline	Baseline	High	—
Q2	40%	– 30%	Medium	Improving
Q3	> 24 hrs	– 60%	Low	Controlled

Tracking TTDD quarterly embeds identity resilience into the governance rhythm rather than treating it as a one-time project deliverable.

9. Executive Diagnostic: Is Your Identity Estate Ransomware-Resilient?

This diagnostic is designed to provide executive clarity, not a technical audit. The questions below translate identity engineering into board-level visibility.

Escalation Density Assessment

Question	Yes	No	Unknown
Do you know the current number of privilege escalation paths to Domain	☐	☐	☐
Is the average hop count to Domain Admin greater than four?	☐	☐	☐
Are direct workstation-to-domain-controller paths eliminated?	☐	☐	☐
Are cross-domain trusts formally reviewed annually?	☐	☐	☐

If two or more answers are No or Unknown, escalation density remains elevated.

Kerberos Governance Assessment

Question	Yes	No	Unknown
Are all privileged SPN service accounts identified and risk-scored?	☐	☐	☐
Is KRBTGT dual-rotation tested and validated?	☐	☐	☐
Is Kerberos anomaly detection integrated with XDR?	☐	☐	☐
Has a Golden Ticket simulation been performed in the last 12 months?	☐	☐	☐

A No in any of the above indicates structural Kerberos exposure.

Domain Controller Exposure Assessment

Question	Yes	No	Unknown
Is Tier 0 administration enforced without cross-tier credential reuse?	☐	☐	☐
Are domain controllers isolated from general-purpose networks?	☐	☐	☐
Are backup administrative identities segregated from production trust?	☐	☐	☐
Is replication boundary scope documented and monitored?	☐	☐	☐

If domain controller isolation cannot be clearly described, DCEI remains high.

Manufacturing And Multi-Site Overlay

Question	Yes	No	Unknown
Are plant-level domain controllers segmented from corporate domains?	☐	☐	☐
Are vendor maintenance identities time-bound and monitored?	☐	☐	☐
Are MES/ERP service accounts reviewed quarterly?	☐	☐	☐
Is TTDD measured separately for plant environments?	☐	☐	☐

Operational disruption risk increases when plant identity boundaries are flat.

TTDD Executive Indicator

Estimate your current Time-To-Domain-Dominance:

Estimated TTDD	Risk Interpretation
< 6 hours	High systemic ransomware exposure
6 – 24 hours	Moderate exposure with containment risk
> 24 hours	Controlled exposure if detection is mature
Unknown	Governance visibility gap

An unknown TTDD indicates the absence of identity modelling discipline.

Diagnostic Summary Scoring

Domain	Status
Escalation Density	Green / Amber / Red
Kerberos Governance	Green / Amber / Red
Domain Controller Isolation	Green / Amber / Red
Manufacturing Segmentation	Green / Amber / Red
TTDD Visibility	Green / Amber / Red

Three or more Red or Unknown indicators suggest immediate need for structured identity risk reduction. This diagnostic is designed to support executive discussion, not replace technical assessment.

10. Operating Model For Continuous Identity Risk Reduction

Identity resilience is not a state that is achieved and then maintained passively. Escalation paths reappear as environments evolve — new applications introduce service accounts, mergers bring in legacy trusts, cloud role mappings expand, and vendor integrations persist beyond their intended scope. Without a continuous governance model, the improvements achieved through a 90-day programme will erode within months.

Quarterly Identity Risk Review Cadence

Review Area	Key Metric	Executive Output
Escalation Path Density	Total paths to Tier 0	Trend line report
Roastable Account Exposure	% privileged SPN accounts	Reduction target update
Domain Controller Exposure Index	DCEI score	Risk band shift
TTDD	Hours	Governance dashboard
Delegation Exceptions	Count	Remediation plan

Quarterly reporting embeds identity metrics into board-level governance cycles.

Change-Driven Risk Reassessment

Identity risk increases when new applications introduce service accounts, mergers add legacy domains or trusts, cloud role mappings expand, or vendor integrations persist beyond project timelines.

Trigger Event	Required Identity Action
New Enterprise Application	SPN privilege review
Domain Trust Addition	Escalation graph recalculation
Cloud Role Expansion	Cross-boundary privilege mapping
Vendor Contract Renewal	Access scope reassessment

No significant infrastructure change should proceed without an identity impact review. The cost of retroactively remediating an escalation path that was introduced by an unreviewed application deployment or domain trust addition is substantially higher than preventing it.

Continuous Simulation Model

Simulation validates that structural controls remain effective.

Simulation Type	Objective
Golden Ticket Exercise	Validate KRBTGT integrity and alerting
Kerberoasting Attempt	Measure roastable account exposure
Lateral Movement Simulation	Test tier enforcement
Backup Compromise Drill	Confirm trust separation

Results should be documented and TTDD recalculated after each exercise. A simulation that reveals a successfully forged Golden Ticket or an undetected lateral movement path is not a failure - it is a finding that should drive the next remediation cycle.

Identity Telemetry Integration

Identity risk cannot be managed through periodic directory review alone. Telemetry integration provides the real-time signal that converts governance discipline into detection capability, making it possible to identify escalation attempts before domain dominance is achieved rather than reconstructing them after the fact.

Data Source	Risk Signal
Kerberos Event Logs	Ticket anomalies
Endpoint Telemetry	LSASS access events
Privileged Access Management Logs	Elevation misuse
Network Segmentation Logs	Cross-boundary movement

Correlation across these sources substantially increases early detection probability. An anomalous Kerberos event that is also correlated with LSASS access on the same host and cross-boundary network movement is a high-confidence signal that warrants immediate investigation. Any one of those indicators in isolation is ambiguous; together they are not.

Executive Accountability Structure

Identity resilience must be assigned clear ownership beyond technical teams.

Function	Accountability
CISO	Identity risk reporting and board updates
CIO	Resource allocation for structural remediation
Head Of Infrastructure	Tier and DC isolation enforcement
SOC Lead	Kerberos anomaly monitoring integration
Business Unit Heads	Vendor and plant identity governance

Clear accountability reduces drift and sustains risk reduction over time. Where ownership is diffuse, identity governance tends to become everyone's theoretical responsibility and no one's actual priority.

11. From Framework To Execution: Governance Imperatives

Frameworks define the problem and structure the response. What determines actual outcomes is whether the organisation executes against the framework with sufficient discipline and authority to make structural change stick.

Identity hardening at enterprise scale requires architectural discipline, cross-functional coordination, and validated simulation. It demands experience in:

- Large multi-domain Active Directory estates
- Kerberos risk modelling and remediation
- Tiered administrative restructuring
- Hybrid identity boundary control
- Plant-level and multi-site segmentation
- Attack-path modelling and TTDD quantification
- Golden Ticket and privilege escalation simulation under controlled conditions

Enterprises that achieve durable identity resilience share common execution characteristics: they treat Active Directory as a risk-bearing control plane rather than a directory utility; they assign quantitative ownership to TTDD and escalation density metrics; and they validate controls through simulation rather than documentation. Execution at this level requires cross-functional discipline. Security architecture, infrastructure operations, SOC, and OT teams must operate against a shared risk model, with governance reporting that holds each function accountable to its segment of the privilege graph.

Identity resilience is not produced by enforced privilege reduction alone, nor by integrated telemetry alone, nor by validated control alone. It requires all three, sustained over time, with accountability structures that ensure none of the three erodes as operational pressures mount.

12. Conclusion: Identity Defence As A Governance Imperative

The Governance Question

When a ransomware event achieves domain dominance, the outcome is determined by decisions made before the attack began. The question for boards and senior leadership is not whether a response plan exists. It is whether the identity estate is structured to limit how far escalation can travel — and whether that limit has been measured.

Ransomware begins with identity compromise. Where escalation paths are short, Kerberos governance is weak, and domain controllers are exposed to general-purpose networks, the scope of a ransomware event is determined within the first hours - before most detection and response programmes have had time to activate. By the point encryption begins, the decisive failure has already occurred.

Recovery planning is essential and should not be abandoned. But recovery plans do not reduce blast radius. Structural identity control does. The two disciplines serve different purposes: identity hardening prevents the escalation that makes a ransomware event systemic; recovery planning addresses the aftermath once it has occurred. Organisations that invest only in the latter are accepting a much larger and more costly event when one eventually arrives.

The governance shift required is from tool coverage metrics to privilege control metrics. TTDD, escalation path density, Domain Controller Exposure Index, and roastable account percentage are the indicators that should appear on risk dashboards alongside financial and operational risk measures. They are neither arcane nor purely technical: they are quantifiable expressions of how exposed an organisation is to the single most consequential phase of a ransomware attack.

For Indian enterprises operating complex multi-site and IT/OT environments, the stakes are higher still. Production continuity, regulatory reporting timelines, and cross-border trust relationships all depend on the integrity of the identity control plane. Treating that control plane as a measurable, governable risk domain - rather than a configuration concern for the infrastructure team - is the strategic shift this guide advocates.

Identity control can be measured. Escalation paths can be reduced. TTDD can be extended. The question is whether the organisation chooses to treat this as a governance priority before an event occurs, or as a forensic finding afterwards.

Appendix

Key Definitions

Term	Definition
Time-To-Domain-Dominance (TTDD)	Estimated time required for an attacker to achieve domain-level authority from initial compromise.
Escalation Density	Total number and length of privilege escalation paths leading to Tier 0 systems.
Domain Controller Exposure Index (DCEI)	Composite measure of administrative surface, replication scope, credential reuse, and monitoring coverage affecting domain dominance probability.
Vendor Identity Risk Index (VIRI)	Structured assessment of vendor privilege scope, duration, segmentation, and monitoring discipline.

Attack Technique Reference

Technique	Risk Category
Kerberoasting	Service Account Credential Exposure
Golden Ticket	Persistent Domain Impersonation
Silver Ticket	Service-Level Forged Access
Pass-The-Hash	Lateral Credential Reuse
LSASS Dumping	Credential Extraction

Metric Reporting Template

Metric	Baseline	Current	Target	Trend
Escalation Path Count				
Roastable Privileged Accounts				
DCEI				
TTDD				
Golden Ticket Simulation				

This guide has set out a practical approach to reducing identity-driven ransomware blast radius in Indian enterprises. The analytical frameworks, the 90-day blueprint, and the governance model all rest on a single underlying premise: that identity risk is measurable, that measured risk can be reduced, and that reduced risk changes outcomes when attacks occur.

Proactive Data Systems is an IT infrastructure and services company that designs, deploys, and supports secure, high-performance technology environments for organisations that cannot afford downtime. With over 35 years of experience, we have enabled more than 1,500 enterprises across India to modernise their networks, strengthen security, and scale with confidence.

Recognised as a Cisco Preferred Partner across Networking, Security, Cloud & AI, and Collaboration, Proactive combines deep systems integration capability with disciplined delivery and managed services. Our expertise spans enterprise networking, cybersecurity, data centres, collaboration platforms, and structured cabling. We build and run infrastructure that performs reliably every day, not just at go-live.

To learn more about our solutions, write to us at pro@proactive.co.in

www.proactive.co.in