Accelerating cyber resilience in corporate transactions with the EY Cyber Factory

Change with confidence

October 2025

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Organizations engaged in large-scale advanced manufacturing and going through separations or transactions across multiple sectors encounter a unique set of critical challenges. In a corporate transaction, separating OT is a high-stakes unbundling of inherited fragility, operational dependencies and decentralized risks.

When cybersecurity is treated as a parallel workstream, the result is often missed TSA milestones, fragmented implementation of controls, and long-term security debt for the new entity. For the newly formed company—NewCo—these risks differ considerably from those typically seen in traditional IT environments:

Time to market and TSA exit

Strict deadlines, often dictated by Transitional Service Agreements (TSAs), raise the stakes. Security must be achieved not just quickly, but sustainably, creating a resilient and independent operation.

Inherited fragility

NewCo inherits a fragile ecosystem of legacy systems and decentralized ownership, often lacking the processes, visibility, and security maturity to manage critical OT assets effectively.

Business disruption

OT systems are built for uptime—any disruption can halt production or trigger safety risks. Unlike IT, the focus is on keeping operations running, not just protecting data.

In the early stages of any strategic transition, CIOs and CISOs face a crucial question:

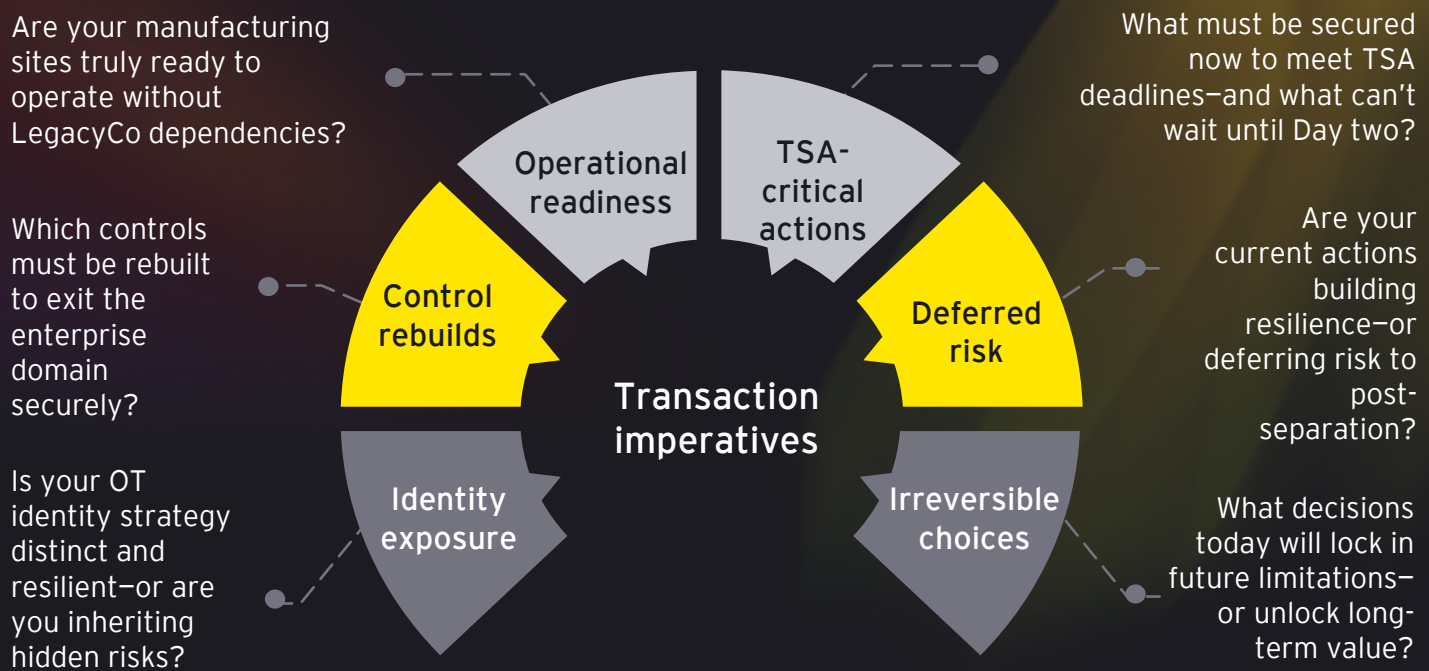
> "How can you support manufacturing site separation that is secure and seamless without disrupting operations or delaying the separation timeline?
>
> – **Kumar Daggubati,** Transformation Program Leader, Ernst & Young LLP

The moment of truth: risk deferred or value captured ?

In every corporate transaction—whether a carve-out, divestiture, or separation—there comes a pivotal moment where security decisions either unlock long-term value or embed future risk.

For CIOs and CISOs, this is that defining moment. As manufacturing site separation gains momentum, security leaders must act decisively—not only to meet core security imperatives like identity boundaries, control rebuilds, and TSA timelines, but to seize the chance to uplift maturity.

This isn't about doing more—it's about doing it smarter. The work is already underway. Embedding resilience now means avoiding costly remediation later and positioning NewCo for autonomy, speed, and modernization from Day One.



How we can help: the cyber separation framework and factory model

The EY Cyber Factory is a structured, repeatable and scalable site separation framework-based model designed to embed resilience from day one. It operationalizes the transaction imperatives—promoting readiness, executing TSA-critical actions and minimizing deferred risk across diverse OT/IT environments. Built around the realities of site diversity, TSA pressure and operational dependency, it helps NewCo operate independently while improving its inherited cyber posture.

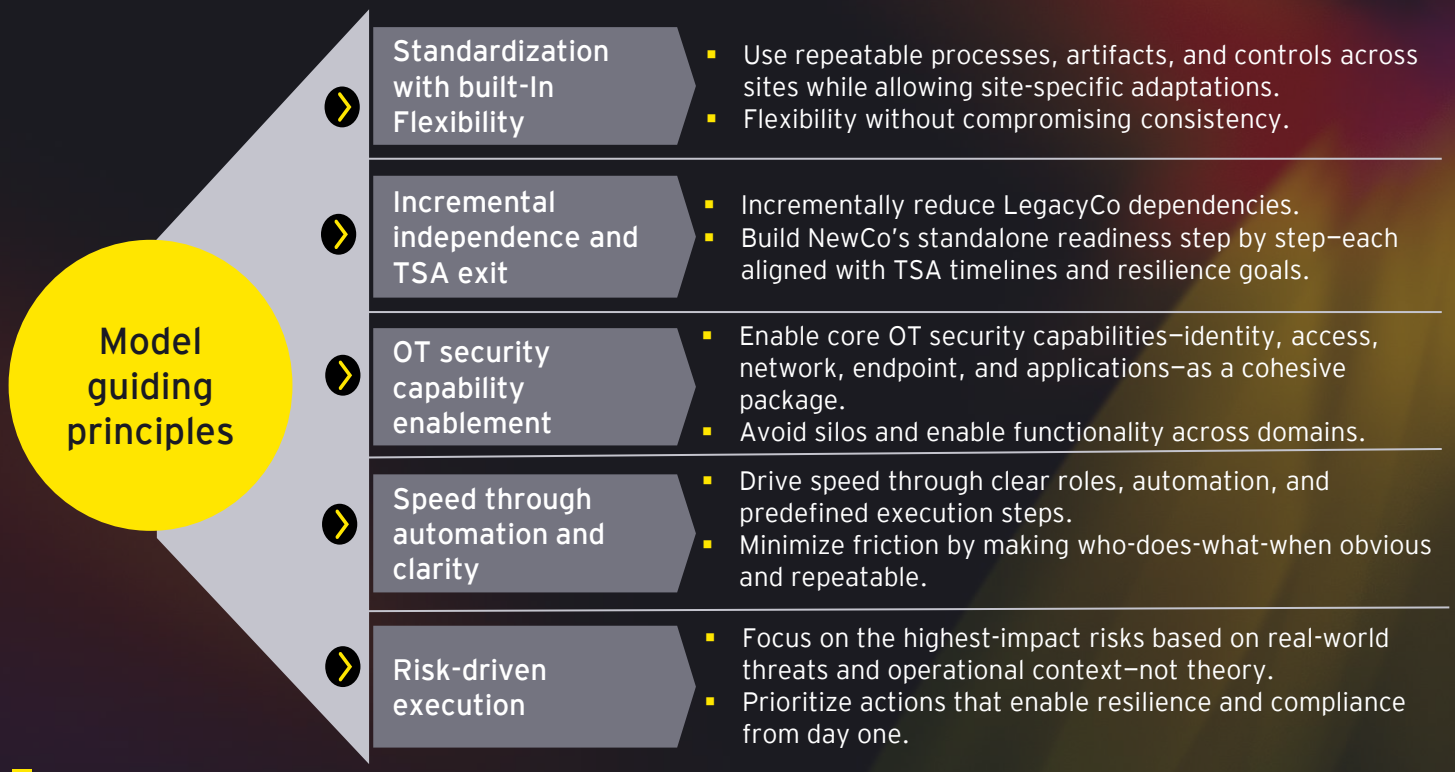
Our Cyber Separation Framework and Factory Model is a proven framework for accelerating manufacturing site cybersecurity readiness. It combines rapid assessments, tailored migration roadmaps and scalable controls—that are already deployed at Fortune 500 spin-offs. This model helps NewCo reduce inherited risk, exit TSAs smoothly and build long-term resilience.

> "The EY Cyber Factory Model treats cybersecurity as part of the conveyance—not a parallel effort—by aligning posture improvement, control execution, and architectural planning into one integrated model."
>
> – **Nagaraj Ganesan,** Transformation Program Leader, Ernst & Young LLP

The EY Cyber Factory Model has delivered significant results for clients. For instance, a Fortune 500 spin-off achieved a 30% reduction in inherited risk and exited TSAs 25% faster than planned. In the advanced manufacturing sector, clients saw a 40% improvement in OT security readiness, enabling operational independence from day one. Additionally, the model's rapid assessments and tailored migration roadmaps have led to a 50% reduction in deferred risk, promoting long-term resilience. These quantitative results demonstrate the model's capability in accelerating cyber resilience during corporate transactions.

Guiding principles behind the EY Cyber Factory Model

The model is shaped by strategic principles, drawn from real-world separation programs:



> "These principles guide each phase of the Cyber Factory Model—delivering consistency, speed, and resilience across NewCo's OT operations.
>
> – **Nagaraj Ganesan,** Transformation Program Leader, Ernst & Young LLP

For the Cyber Factory Model to scale across diverse OT sites, it requires more than execution discipline—it demands architectural scaffolding. Architectural scaffolding that supports migration, maturity, and risk reduction. This foundation aligns teams, standardizes activities, and turns one-off security uplift into a repeatable delivery engine.

The structural core of cyber readiness

This factory-style model integrates architectural scaffolding, execution discipline, and separation planning into a single lifecycle. It avoids theoretical maturity models in favor of site-ready controls, standardized artifacts, and practical implementation paths—helping NewCo achieve operational independence within compressed timelines, without compromising security.

Our approach embeds these preparatory steps to support factory-model orchestration:

Site-level blueprints

Map OT systems, dependencies, and posture to accelerate secure control rollout and prioritization.

Gap identification and remediation planning

Identify inherited risks and plan remediation aligned with migration.

Future-state architecture definition

Design NewCo's end-state aligned to risk and modernization goals—used as the anchor for all control decisions.

EY CYBER FACTORY

Standardization for scale

Codify controls and readiness playbooks to scale security with speed and consistency.

TSA-aware migration integration

Integrate remediation into site transitions – aligned with TSA timelines and business continuity.

Control-to-architecture alignment

Align controls to future-state architecture to validate coverage and eliminate overlaps or blind spots.

> "By making cyber part of the transaction lifecycle — and treating each site as a production line within a broader factory — the Cyber Factory Model brings both predictability and resilience to a process often defined by uncertainty and compromise."
>
> – **Rakesh R Panati,** Innovation & Advisory Architect, Ernst & Young LLP

Delivering cyber readiness in phases

A factory model built to mirror how organizations approach corporate transactions—from spin-offs and divestitures to functional and site transitions.:

Phased Cyber Enablement

Engage, Walkthrough & Gap Identification

- Cyber team presents the Cyber Factory Model and site execution plan during kickoff
- Site Controls team performs site walkthrough, collects asset, identity, and access data
- Gaps are identified in current controls, local admin/service accounts, and AD structures
- Application inventory begins, differentiating IT vs OT with input from site teams

Architecture & Segmentation Design

- Identify what's unique about the site across devices, network, infrastructure, supply chain, and OT applications to inform segmentation and remediation planning
- Leverage findings to align with Purdue Model and ISA/IEC 62443 as reference

Application Profiling & Control Structuring

- EY AppON platform is used to gather structured app data and dependencies
- Controls (identity, endpoint, access) are aligned to business impact and site readiness
- Profiles inform security zoning, access decisions, and remediation priorities

Embedded Remediation & Execution Planning

- Identified gaps are converted into tasks aligned with conveyance milestones
- Activities span IAM, segmentation, endpoint protection, remote access, and firewall hygiene
- Controls are implemented in coordination with site teams, minimizing operational impact

Cross-Checkpoints, Handoff & Documentation

- Milestones drive coordination across cyber, infra, and conveyance teams
- Final site handoff includes validated controls, updated architecture, and segmentation in place
- All exceptions, POAMs, and known residual risks are documented and transferred to NewCo

Cyber Factory capabilities: from objectives to realized value

The Cyber Factory transforms corporate transactions complexity into a structured path for OT security execution. Each embedded capability is designed to meet a specific separation objective—whether establishing identity boundaries, validating inherited assets, or deploying scalable controls. These are not theoretical best practices—they are delivery-tested components that enable NewCo to take ownership of its OT environment with clarity, autonomy, and resilience.

#	Key focus areas	Objectives	Value realized
1	Active Directory (AD) Management	Establish a standalone, secure AD environment for NewCo, including OU design, GPO validation, and removal of legacy dependencies.	Seamless domain migration with minimal disruption; PKI integration completed; foundational controls in place for Day 1 operations.
2	Identity & Access Management (IAM) and Governance (IGA) for OT	Implement identity-based access for OT users and assets; eliminate shared credentials; enforce least-privilege access.	Strengthened OT access control posture; privileged access secured via CyberArk; improved auditability and compliance readiness.
3	PKI and Certificate Management	Establish a secure, scalable PKI structure to support OT authentication and encrypted communications.	Enabled certificate-based authentication for OT systems; reduced risk of expired or unmanaged certificates.
4	Firewall Policy Management and Segmentation	Redesign firewall rules based on validated communication flows; implement secure remote access aligned with segmentation strategy.	Reduced attack surface through active rule management; centralized control of security zones; improved visibility and enforcement.
5	Accelerated OT Application Security Review	Rapidly inventory and assess OT applications across sites; identify critical apps for prioritized protection and IAM integration.	Application landscape mapped ahead of schedule; high-risk apps integrated into IAM; accelerated readiness for OT security controls.
6	OT Asset Visibility and Continuous Monitoring	Deploy tools and processes to discover, classify, and monitor OT assets in real time.	Improved visibility into OT environments; enabled proactive risk detection and response.
7	OT Cyber Control Framework Realization	Translate OT security policies into actionable, site-ready controls aligned with industry standards.	Accelerated implementation of OT controls; improved audit readiness and compliance alignment.
8	OT Threat Detection and Response (TDR)	Implement OT-specific threat detection and incident response capabilities.	Enhanced detection of anomalous behavior; reduced mean time to respond (MTTR) to OT threats.
9	OT Security Architecture via Systematic Assessment	Conduct structured assessments to define and validate OT security architecture across sites.	Delivered a consistent, risk-aligned architecture blueprint; informed control deployment and investment decisions.

> “These capabilities are not theoretical—they are delivery-tested components that enable NewCo to take ownership of its OT environment with clarity, autonomy, and resilience.
>
> – **Ankit Yadav,** Enterprise Transaction Architect, Ernst & Young LLP

Cyber resilience: the strategic edge in corporate transactions

Cybersecurity in the context of a corporate transaction is not simply a defensive measure—it is a foundational enabler of operational independence. By embedding security activities into the separation process, NewCo avoids inheriting technical debt and gains a clear trajectory toward sustainable resilience. The EY Cyber Factory accelerates this shift by front-loading core security capabilities into the timeline that matters most: before TSA constraints expire and governance fragmentation sets in.

> “This transition—from inherited complexity to operational clarity—is not a byproduct of separation. It must be deliberately designed.
>
> – **Avdesh Mishra,** Strategic Solutions Leader, Ernst & Young LLP

Establishing identity boundaries, zoning critical networks and validating control implementations are not optional. They are prerequisites for standing up a secure, autonomous OT operating environment.

The benefits are tangible:

Front-loading security investment avoids the significantly higher costs and operational disruption of post-separation remediation projects.

Security gaps are addressed early, minimizing exposure from legacy systems and misaligned access.

NewCo meets TSA milestones without compromising on foundational controls.

A future-ready architecture is established—positioning NewCo for modernization efforts including IIoT integration, Zero Trust adoption, and cloud-enabled innovation.

Operational autonomy is achieved, reducing future reliance on LegacyCo infrastructure and resources.

Ready to see these benefits in action? Contact us to schedule a live demonstration of the EY Cyber Factory Model and discover how we can accelerate your organization's journey from risk to resilience. Let’s start a conversation about your unique needs.

> “In a spin-off, cybersecurity isn't just about protecting what you inherit—it's about shaping what you become. By embedding security into the architecture of separation, we help NewCo's move faster, reduce risk earlier, and operate with clarity from day one.”
>
> – **Avdesh Mishra,** Strategic Solutions Leader, Ernst & Young LLP

Meet our Ernst & Young LLP team

Avdesh Mishra
Strategic Solutions Leader,
Technology Consulting

Kumar Daggubati
Transformation Program Leader,
Technology Consulting

Nagaraj Ganesan
Transformation Program Leader,
Technology Consulting

Rakesh R Panati
Innovation & Advisory Architect,
Technology Consulting

Ankit Yadav
Enterprise Transaction Architect,
Technology Consulting

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

2509-11907-CS
ED None

ey.com