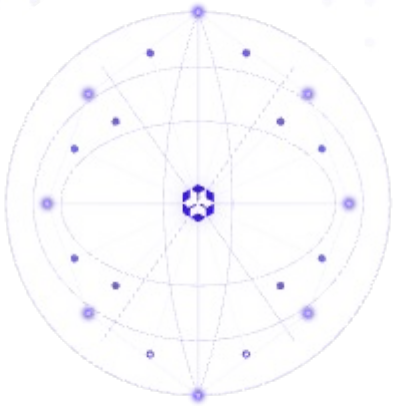
ASTRAN



RECOMMENDATION REPORT

For CEOs, Boards and Resilience Leaders

Business Resilience

The Minimum Vital Company framework

MARCH 2026

Agenda

Executive Summary

Why defining the Minimum Vital Company (MVC) is critical

What it takes to make a Vital Activity executable

The 5 Vital Activities framework

Priority focus: Be able to make Critical Payments

Implementation in 3 phases

Governance & Decision-making, the role of the Resilience Leader

Conclusion

Executive Summary (1/2)

In a major disruption scenario (cyberattack, prolonged IT outage, infrastructure failure, kill switch of US's apps, etc.) **resilience is not about maintaining everything; it is about preserving viability.**

Defining the MVC: The Minimum Vital Company defines the smallest set of processes and data that must remain executable to ensure organizational survival. It shifts resilience from documentation to execution.

Most large organizations have invested significantly in Business Continuity Plans (BCP), Business Impact Analysis (BIA), and crisis documentation. Yet when primary systems become unavailable, when data integrity is uncertain and when time pressure escalates, many discover a structural weakness: they know what should happen, but they cannot reliably execute it.

What makes a Vital Activity executable? Two elements must be simultaneously available, protected and tested:

- An **executable process** meeting the following requirements: simplified, self-sufficient (no ERP/cloud/IT reliance), built around named roles with enforced separation of duties, and regularly micro-simulated
- **Vital Data** extracted regularly, stored independently, integrity-validated, and accessible at any time.

The 5 Vital Activities framework

1. Keep the Core Service running
2. Customers get served and monetized
3. People and Sites stay protected
4. **Be able to make Critical Payments**
5. The company communicates and stays compliant

Executive Summary (2/2)

Each organization should limit itself to a maximum of 10 Vital Activities. Beyond that, the framework loses its disciplining effect. Each Vital Activity then breaks down into executable processes, keeping the overall structure manageable and actionable.

Where to start: with Critical Payments. Financial paralysis occurs before operational paralysis: Treasury is process-intensive, data-driven and connects HR, Finance, Procurement and Banking. It is the entry point to build the cross-functional coalition for broader Minimum Vital Company rollout.

Implementation in 3 phases

- **Phase 1: Build one end-to-end process** in one entity, mapping every step, role, data input and decision point, extract and store Vital Data.
- **Phase 2: Test under simulated crisis conditions** without primary systems. Testing is the only proof of executability.
- **Phase 3: Scale and replicate to other critical entities and geographies**, using the first process as a template.

Governance: The CISO or Resilience Leader must sit at executive level. **Minimum Vital Company empowers the executive committee with a project that takes back control over the fate of the whole company**, and makes Finance and Resilience executives work together for a strong common objective.

Resilience must be measurable, structured, and operational – not theoretical.

Why defining the Minimum Vital Company (MVC) is critical

The Minimum Vital Company represents the minimal operational core of an organization during severe disruption. It includes only what cannot stop without threatening company survival.
Some refer to this as Important Business Services (IBS), others speak of critical functions or essential activities. Terminology varies, but the exposure does not.

The limits of traditional BCP

Traditional business continuity approaches share a common assumption: that the organization will have time, information, and system access sufficient to orchestrate a structured response. In a prolonged cyber-driven disruption, none of these assumptions hold.

Static plans fail because they describe what to do without building the capacity to execute it when normal infrastructure is unavailable. They were never designed to be operational.

What changes with the Minimum Vital Company

The Minimum Vital Company addresses this exposure by forcing prioritization.

It requires leadership to **distinguish between important and existential,** and to identify the processes that must remain executable even when primary systems are unavailable.

Defining the Minimum Vital Company forces three decisions that traditional BCP avoids:

- Which activities are existential
- Which simplified processes can execute those activities under alternative conditions (without relying on ERP, cloud or central IT systems)
- Which minimum datasets must be available, protected and current to support those processes.

The Minimum Vital Company transforms resilience from reactive crisis management into structured efficiency: instead of asking “How do we recover everything?”, the organization asks “What must we preserve to survive?”.
Organizations that have documented their Minimum Vital Company without building executable processes and protected data are, in practice, no more resilient than those with no Minimum Vital Company at all. The documentation creates a false sense of readiness.

What it takes to make a Vital Activity executable

Defining a Vital Activity is not the same as being able to execute it. This distinction is the most commonly underestimated gap in resilience programs.

An activity becomes executable in crisis conditions only when two elements are simultaneously available, protected and tested: a process and the associated data.

The executable process

An executable process is not a replica of a normal operation; it is an intentionally simplified or alternative version, designed to produce essential outputs without relying on primary IT systems. It must be simple enough to be executed by a limited crisis team while staying fully aligned with the company's compliance requirements.

The process must:

- Be executable by named individuals with clearly defined roles and decision authority (Separation of Duty)
- Function without ERP, cloud-based orchestration or IT support (independent)
- Have been tested under conditions that simulate genuine deterioration (simulated)

The independence requirement is essential.

If a process requires the primary ERP to retrieve inputs, the corporate network to transmit approvals or the cloud to store outputs, it is not a fallback one.

The Vital Data

Every executable process requires data. In critical conditions, that data must be available through means entirely independent of primary systems.
Vital Data are the minimum datasets required to execute and make decisions safely and compliantly.

They must be:

- Extracted from primary systems at regular intervals, consistent with business tolerance thresholds
- Stored independently, and protected against encryption or corruption
- Validated for integrity at each extraction
- Accessible to the right individuals under crisis conditions (including when corporate authentication systems are unavailable)

Defining what data is vital, how often it must be refreshed, and who can access it is a business continuity decision that must be made before a crisis occurs.

The 5 Vital Activities framework

Resilience becomes actionable when structured around 5 universal categories of Vital Activities. Although terminology differs across industries, the fundamental logic remains the same: certain domains of activity are essential.

These categories typically include:
1. Keep the Core Service running
2. Customers get served and monetized
3. People and Sites stay protected
4. Be able to make Critical Payments
5. The company communicates and stays compliant

The Executive Committee is responsible for defining the organization's Vital Activities per category, in their own words. These are the activities that must be maintained no matter what. Each relevant Head of Business Unit then picks up from there, identifying which Critical Processes within their scope support each Vital Activity.

Each organization must define their specific Minimum Vital Company. In practice, it means selecting 2 to 3 Vital Activities per category and translating them into executable processes. These processes will represent what an organization cannot survive without.

1. Keep the Core Service running

→ Continuity of critical production and service delivery activities

Delivering the Core Service is what customers, regulators and partners perceive first. Yet in a severe disruption, maintaining full operational capacity is unrealistic. The objective is not to preserve performance levels, but to preserve essential output.

Core service continuity means identifying which production lines, service modules, platforms, or transaction flows are existential, and which can be temporarily suspended without threatening survival.

Typical exposure areas include:

- Raw material sourcing
- Manufacturing operations
- Inventory management
- Distribution and logistics
- Clinical trials
- Transaction processing

In disruption scenarios, dependencies become visible: supplier concentration, single-site production, reliance on ERP-driven planning or cloud-based orchestration.

2. Customers get served and monetized

→ Maintain customer engagement, service execution and revenue continuity

Revenue erosion during disruption is rarely immediate, but it accelerates when customer interaction collapses. If customers cannot place orders, submit claims or receive responses, confidence deteriorates quickly.

Serving and monetizing customers in Minimum Vital Company mode means ensuring that the organization retains its ability to transact.

This includes:

- Customer support
- Claims management
- Sales and tender responses
- Order management
- Invoicing and cash collection
- Patient “management”

Customer continuity protects not only revenue, but reputation. In many industries, the way an organization communicates and transacts during a crisis shapes long-term market perception more than the disruption itself.

3. People and Sites stay protected

→ Maintain workforce availability and protect sites and critical assets

Operational recovery is impossible without human and physical stability. In many crises, confusion spreads rapidly: employees may lose access to systems, site access controls may malfunction. Protecting People & Sites is therefore foundational as it ensures that the organization remains physically and organizationally intact.

This includes:

- Remote work capability
- Workforce reallocation
- Site access control
- Health and safety procedures
- Physical asset protection

The focus is ensuring that critical roles remain staffed and that essential decision-makers are reachable.

For physical sites, it must define which locations are critical, and clarify how access is controlled if digital badges fail, how safety reporting continues and how essential equipment is secured.

4. Be able to make Critical Payments

→ Ensure execution of high-priority financial obligations

It is the most widely adopted Vital Activity across industries, and the recommended starting point (see next chapter for more details).

In prolonged disruption scenarios, financial paralysis often occurs before operational paralysis. If payroll cannot be processed, strategic suppliers remain unpaid or debt and tax obligations are missed, confidence deteriorates rapidly both internally and externally.

Process candidates include:

- Payroll
- Critical supplier payments
- Tax payments
- Debt servicing
- Inter-company balancing

The key is to ensure that essential obligations can be executed independently of primary ERP systems.

This requires predefined priority lists, isolated and secure access to banking channels, validated signatory continuity, and independent visibility over minimum liquidity data.

5. The company communicates and stays compliant

→ Maintain structured communication and meet regulatory obligations

In crisis, silence creates speculation, inconsistent communication creates mistrust and missed regulatory filings create legal exposure. This Vital Activity ensures that the organization retains structured narrative control and legal standing during disruption.

This includes:

- Crisis communication
- Executive and board reporting
- Regulatory filings
- Incident notifications
- Investor and partner updates

Communication must be centralized, validated and supported by reliable information. Executive teams must retain access to decision-grade data, even if simplified.

Astran expert view

Every organization is different with its critical processes, dependencies, and tolerance thresholds that reflect its business model and operating context. **Companies should not exceed 10 Vital Activities.**

Priority focus: Be able to make Critical Payments

While the Minimum Vital Company ultimately spans multiple domains, implementation must begin where exposure is most immediate. **Critical Payments represent the most pragmatic and structurally stabilizing starting point.**

In a prolonged disruption scenario, ERP systems may be unavailable, banking connectivity may be partially impaired, cash visibility may be fragmented and signature authorities may be unreachable.

Finance and Treasury are not an administrative function; it is a survival function.

By securing Critical Payments first, the organization stabilizes its workforce, preserves supplier relationships, maintains financial credibility and buys time to restore other Vital Activities. Financial continuity becomes the anchor that allows operational recovery to proceed in an orderly manner.

“Be able to make Critical Payments” Vital Activity also offers a structural advantage as a starting point; it is inherently process-intensive and data-driven.

It connects HR, Procurement, Finance, Banking partners, and executive leadership. **Building the Minimum Vital Company through this Vital Activity creates the cross-functional coalition required for broader rollout.**

In governance terms,

- Both the CISO/Resilience Leader and the Head of Treasury emerge as natural co-owners of Minimum Vital Company implementation
- Treasury identifies critical financial processes and required datasets
- The CISO/Resilience Leader maps system dependencies, secures fallback environments, and ensures the integrity of Vital Data
- Executive accountability typically rests with the COO, ensuring alignment across operational domains.

Implementation in 3 phases

Building the Minimum Vital Company is an operational build, one process at a time, validated before being scaled. For each Vital Activity selected, implementation follows three phases:

Phase 1: Build the first end-to-end process

Select the highest-priority critical process within the Vital Activity (eg: Critical payments, Payroll, etc.), and map it end-to-end. Every step, role and data input required must be mentioned, in addition to every decision point and output. All dependencies on primary systems must be identified, and the fallback equivalent that can run without them designed.

Simultaneously, organizations must define and extract the Vital Data required to support this process and establish the storage environment, refresh frequency and access protocol. **It is essential to validate that the data is complete, current, and accessible under crisis conditions.**

At this stage, **the focus must remain entirely on a single process, in one critical entity or geography.**

Phase 2: Test and validate

Organizations must execute the process under simulated crisis conditions (without primary systems, normal authentication or ERP), and document what is working and what is not.

The process can then be refined until the execution is reliable. Testing is the only proof of executability.

Phase 3: Scale to critical entities and geographies

Once reliability is demonstrated, the process can be validated and replicated. Organizations can then expand to other critical entities and geographies. The first process is a template: the process design, data architecture, and governance model do not need to be reinvented, but adapted and retested.

Governance & Decision-making, the role of the Resilience Leader

Modern disruptions are increasingly cyber-driven. As a result, resilience governance must integrate cybersecurity leadership at executive level.

The CISO/Resilience Leader plays a central role in Minimum Vital Company governance for three reasons:

- Cyber incidents are now a primary cause of prolonged operational disruption
- All Vital Activities depend on systems availability and data integrity
- Alternative execution environments must be secured and isolated.

The CISO/Resilience Leader contributes to identifying critical system dependencies, protecting Vital Data from corruption or encryption, validating fallback architectures, and ensuring that simplified processes remain secure under critical conditions.

Resilience is no longer solely operational; it is a strategic and cyber governance matter.

Effective Minimum Vital Company governance requires coordination between all teams: Treasury, Operations, Risk & Compliance, IT, CISO (or Resilience Leader) and Executive Committee.
The CISO/Resilience Leader is a key decision-maker in determining what must remain secure, accessible and executable.

Critically, the CISO or Resilience Leader must be involved upstream; their role in defining the Minimum Vital Company, validating its independence from compromised infrastructure, and stress-testing its security assumptions is foundational and must be engaged at design stage.

Conclusion

Operational survival during major disruption requires clarity, prioritization, and governance discipline. The Minimum Vital Company forces organizations to confront a decisive question: what truly cannot stop?

By defining the Minimum Vital Company, structuring resilience around Vital Activities, securing Critical Payments capabilities, integrating the CISO or Resilience Leader into executive decision-making and enabling independent execution environments, organizations move from planning resilience to executing it.

Organizations that do this work in advance hold a structural advantage. They know their Minimum Vital Company works because they have proven and acted on it.

Resilience is not about maintaining everything – it is about ensuring that what truly cannot stop does not, even when primary systems fail.

Download the pdf version here:

About Astran

Yosra Jarraya
Co-Founder
Chief Executive Officer

Yahya Jarraya
Co-Founder
Chief Customer Officer

Gilles Seghaier
Co-Founder
Chief Technology Officer

Astran delivers **Minimum Vital Company as-a-Service: the platform that keeps Vital Activities running when primary systems go down.** Ransomware, outages, and supplier failures don't just disrupt IT. They freeze Important Business Services for weeks.

Astran solves the execution gap. AlwaysReady® lets companies define, synchronise, and run their critical processes independently of primary infrastructure, step-by-step. From day one of a crisis. The result: critical operations continue while IT recovers.
The platform is operational, controlled, and fully independent. Its patented cryptographic architecture combines All-Or-Nothing Transform with Threshold Secret Sharing. No single point of compromise. No encryption keys to steal. This is structural, not a feature.

Your Vital Activities run. No matter what.

ASTRAN

Be AlwaysReady®

Your vital activities run. No matter what.
Minimum Vital Company as-a-service

21 rue de Bruxelles
75009 PARIS

hello@astran.ai

www.astran.ai