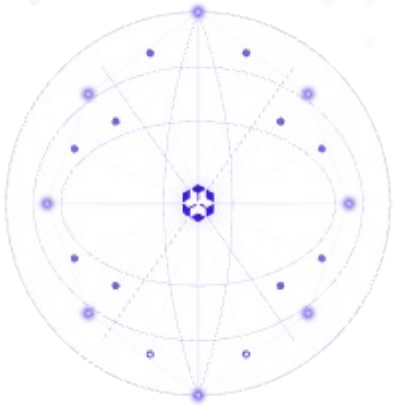
ASTRAN



RECOMMENDATION REPORT

Treasury Resilience: building an effective action plan

In Collaboration with Future of Finance

MARCH 2026

Agenda

Executive Summary

Treasury Resilience requires a focused, cross-functional approach built around three pillars:

Protect what matters most. The Minimum Vital Company (MVC) framework identifies the restricted scope of processes that must remain executable under all circumstances. In the case of Critical Payments, this would be: salary payments, critical supplier payments, or core Treasury operations.
Mapping these processes reveals significant optimization opportunities, on average, 30% of applications and 50% of reports prove to have little real value.

Assume your tools will be unavailable. Cloud-based TMS, authentication systems, and standard access channels may all be inaccessible during a major crisis. Resilience depends on pre-identified backup banking arrangements, independently stored critical data, and procedures executable from day one, without primary infrastructure.

Make it a business decision, not a technical project. Treasury Resilience must be arbitrated at Executive Committee level, with a cross-functional coalition (Finance, IT, Cybersecurity, Procurement) and a business case grounded in operational consequences.

Five principles to get started

1. Assume total outage for 24 days**
2. Prioritize a limited process scope
3. Involve a small, identified team
4. Start with one end-to-end process
5. Test regularly

Editorial

When Treasury stops, everything stops. Essential financial commitments are no longer honored: salary payments, critical suppliers payments, debt servicing, and group cash flows.

Such a situation is untenable. Yet major companies such as Marks & Spencer and Jaguar Land Rover have recently experienced it.

The growing dependence on information systems now exposes finance departments to systemic risk. **In the event of a major cyberattack or the failure of a critical provider, the Treasury function may no longer be able to carry out its vital missions. In this context, identifying priority payments, executing payments reliably, and verifying bank details become immediate operational challenges.**

This loss of control can lead to a total paralysis of the organization, generating significant financial impacts and a rapid erosion of trust among partners, employees, and markets.

For this reason, around fifteen Treasury directors from major French groups met as part of the **Treasury Resilience and Efficiency Taskforce**. Their shared objective: **establish an effective action plan to ensure Treasury Resilience.**

To achieve this, they worked together on several key questions:

- Which critical business processes must never stop (salary payments, debt servicing, strategic suppliers)?
- How can vital data remain available when usual tools, including cloud-based tools, are no longer accessible?
- Which banking relationships should be prioritized in a crisis: multiple banks versus a single strategic bank dedicated to certain processes?

Editorial

- How can a solid Business Case be built to convince the Executive Committee to invest in Treasury Resilience?
- Which strategic allies should be engaged (cybersecurity, procurement, banks, internal control), and how can they be convinced?
- How can a Digital Resilience Business Case (DRBC) be used as a common foundation between the Treasurer, the CFO, and external partners?

While this report cannot provide a tailored answer to every specific context, the working group's ambition was to offer clear and accessible recommendations. **They are intended to enable each organization to define an appropriate action plan, ensuring that vital Treasury processes are never interrupted.**

– **Yosra** **JARRAYA**
Astran CEO & Co-founder

#1

Workshop
Treasury Resilience

From Business Case to Strategic Alliances

Treasury Resilience: from Business Case to Strategic Alliances

The Taskforce's work highlights the need to strengthen awareness of cyber risks affecting Treasury.

Treasury Resilience cannot be treated as a strictly financial matter. It requires mobilizing all key stakeholders from the outset, whose composition may vary depending on the organization (finance, IT, cybersecurity, operations, procurement).

In most participating companies, the Executive Committee member empowered **to arbitrate and drive a Treasury Resilience strategy** is the Chief Financial Officer (CFO), and in some cases the Chief Operating Officer (COO). Their decision relies on the business expertise of the Treasury function, in close collaboration with the Cyber department, which is responsible for overall Resilience. The CFO (or COO) also arbitrates budget allocation in line with internal policies: certain costs may be borne by IT or cybersecurity (licenses, solutions), while implementation and support may fall under finance, operations, or cybersecurity depending on the case.

To avoid dispersion and maintain budget control, the Taskforce recommends a pragmatic approach consisting of **protecting only the company's Vital Processes**, without attempting to replicate the entire information system. This logic, referred to as the Minimum Vital Company (MVC), is based on a simple analysis: measuring the impact that a major cyber crisis - whose average duration is estimated at 21 days* - would have on each process. This method enables the construction of an effective business case, grounded not in a theoretical ROI but in the concrete operational consequences of a Treasury paralysis.

Participants agreed on three vital processes within the Treasury function: **salary payments, critical suppliers payments, and "pure Treasury" processes.**

Finally, the work emphasizes that Treasury Resilience is also a lever for transformation. Mapping processes, flows, and systems not only helps secure existing operations, but also simplifies the organization, identifies truly critical data, and strengthens governance. In this respect, **Treasury protection must be driven and arbitrated at the Executive Committee level as a strategic decision related to business continuity and risk management - not as a mere technical project.**

Internal engagement: When Treasury protection becomes a driver of transformation

Assessing the impact of a crisis on Treasury operations

Ransomware attacks generate prolonged business disruptions and significant financial impacts, as illustrated by two major incidents in 2025: Jaguar Land Rover (cyberattack) and Marks & Spencer (ransomware).

DOWNTIME	
JAGUAR LAND ROVER **± 6 weeks**	MARKS & SPENCER **± 46 days**
DIRECT COSTS	
JAGUAR LAND ROVER **196M£**	MARKS & SPENCER **300M£**
FINANCIAL IMPACT	
JAGUAR LAND ROVER **11% of 2024/2025 profit**	MARKS & SPENCER **30% of margin** (1/3 of forecast profit)
SYSTEMIC IMPACT	
JAGUAR LAND ROVER **State-guaranteed credit facility: £2Bn, -0.1% UK GDP (Q3 2025)**	MARKS & SPENCER **Impact on margins and EBITDA**

These incidents illustrate how a single cyber event can significantly impact the financial and operational performance of large corporations, with repercussions extending beyond the company itself. Industry context: average downtime of 21–24 days (Coveware*, Statista**), average IT downtime cost: USD 5,600 per minute (Gartner***).

Workshop #1

To raise awareness of cyber risks affecting Treasury, teams must enable everyone to fully grasp their magnitude. However, quantifying the financial impact of a cyber-induced Treasury shutdown in order to build a business case remains difficult at this stage. The impact of a production shutdown is often quantified by companies, notably through Business Impact Analyses conducted by the cyber team. It is also possible to base calculations on the average duration of a cyber crisis (21 days*) applied to the company's daily revenue. Yet there is no specific "Treasury" component in these assessments.

In this context, listing the potentially devastating effects of a cyberattack specifically on Treasury provides a clear understanding of what is at stake.

- Risks to the supply chain and supplier payments (risk of loss of trust, or even disruption, with critical suppliers)
- Risks to sales and market share due to inability to deliver (inability to pay carriers, retailers, and other intermediaries essential to the sales process)
- Legal impact resulting from non-compliance with commercial and financial contracts
- Major social risk in the event of disruption of essential payments, particularly salaries, whose internal visibility makes them a powerful lever for awareness
- Reputational risks and threats to the company's insurability (conversely, effective protection strengthens negotiating power with insurers).

**Coveware (2020) – 21 days average downtime (Coveware Q4 2020 Ransomware Marketplace Report)*

***Statista (2024) – 24 days average downtime (based on surveys measuring the average duration of disruption following a ransomware attack)*

****Gartner (2014) – average IT downtime cost estimated at USD 5,600 per minute (Gartner IT Downtime Cost Study)*

Engaging all stakeholders, identifying critical processes and suppliers

With this list, it becomes clear that Treasury protection must move beyond the strictly "Finance" zone and mobilize the entire organization around two essential tasks: identifying critical processes and the indispensable suppliers that must be protected as a priority.

Bringing all stakeholders together requires informing them about the role of Treasury through a clear, end-to-end description of financial processes.

Another key point is to ensure that each function's area of expertise is respected. The Treasurer must not attempt to act as a cybersecurity expert, at the risk of creating friction with IT or the Cyber department (depending on the organization), which are identified as essential partners in implementing effective protection.

Recommendations

- **Building and presenting concrete crisis scenarios** is an effective lever, and Treasury crisis simulations, when feasible, produce compelling results.
- **Turning to partner companies** for potential feedback and shared experience.
- **Insurance premiums** are identified as a relevant entry point for discussions with Procurement.
- It may be necessary to conduct a form of internal "corporate geopolitics" to identify the most influential function at the Executive Committee level (outside Finance).
- **Identify tangible benefits for each stakeholder,** particularly through transformation opportunities.
- For IT teams, the strongest argument is that a Treasury function capable of operating despite an attack allows them to focus fully on restoring production systems.

Transformation lever

This is an aspect that must not be overlooked when building a business case for Treasury protection and triggering investment.

Protecting Treasury and implementing backup solutions to mitigate the impact of a cyberattack requires a comprehensive mapping of the systems and applications used by the company.

During a detailed review, **on average 30% of applications and 50% of reports prove to have little real value**. The potential savings identified through this assessment often largely finance Treasury protection initiatives.
A precise identification of critical processes can also lead to more effective protection across the entire production chain.

Similarly, a detailed review of processes helps identify the “golden data” that can become powerful drivers of value creation.

Astran expert view

The challenge is not to maintain all activities, but to identify what must absolutely continue to operate in order to ensure the company’s survival.

The Taskforce’s work shows that Treasury emerges as one of the most critical processes. This approach aligns with the concept of the **Minimum Vital Company (MVC)**: a restricted scope of processes and data that must be preserved under all circumstances.

Defining this MVC makes it possible to prioritize efforts, anticipate crises, and organize a degraded yet controlled mode of operation - an essential condition for both Treasury Resilience and overall corporate Resilience.

We cannot simply wait, we must prepare effectively. That is why I firmly believe that decisions and communications on these matters must be made at the Executive Committee level.

Thierry Revah

Director Financing & Treasury TP

Interview: Thierry Revah, Director Financing & Treasury TP

TP, formerly Teleperformance, is the global leader in outsourced customer experience management, operating worldwide with significant real-time response requirements and a very large workforce (around 500,000 employees). This undoubtedly makes Treasury-related issues even more critical. My first question follows from this observation: are threats to Treasury addressed by cybersecurity teams in the same way as those directly affecting production?

I would say that recent cyberattacks, increasingly high-profile - such as those that hit Jaguar and Marks & Spencer - have only heightened the awareness of the Executive Committee and the group's leadership regarding these risks. Given the very nature of our business, we are already highly conscious of these threats, but it is crucial that we remain vigilant and proactive.

Specifically regarding Treasury, we are now facing increasingly sophisticated fraud attempts, including highly realistic deepfake Teams sessions in which our CEO appears to request specific transfers to specific countries, often China. This happens several times a week.

The level of sophistication is such that the mobilization and communications required to resist these attacks are now managed by the cybersecurity teams, whereas in the past Treasury could handle them independently.
I know my limits, I can no longer handle such a deluge of attacks and such a high level of sophistication. And I believe this is a very important point in our discussion: **organizing Treasury protection requires involving the entire company**.

The other key point is that sophisticated tools are needed, which brings us to the question of investment.

Indeed, that was at the heart of our community's discussions: how do you build a business case strong enough to secure the necessary investment?

I would say the first step is not to talk about budget at all. Our working group concluded that it is almost impossible to quantify the financial impact of a Treasury paralysis. And that is actually a good thing, because it allows us to focus on the real consequences - and they are devastating.

At TP, non-payment of salaries leads to very serious situations very quickly. It has happened to us, due to technical issues in certain countries, to be one or two days late in paying salaries - and strikes were immediate. Just as quickly, our clients, who require real-time responses, shift their traffic to competing platforms. Everything moves extremely fast.

I must also say that I was struck by the massive power outage in Spain. In such cases, the solutions are relatively simple to formulate: decentralize and maintain the ability to operate from different parts of the world to deal with such incidents. Simple to articulate, but complex to implement, and it is therefore a major initiative that we are currently undertaking.

Returning to budget discussions, I insist that we should not be looking for an ROI, but rather consider this as a form of insurance premium that ensures business continuity.

Because the stakes are too high.

Exactly. And I would add the transformation opportunity, which I discovered through our discussions.

What are our truly critical processes? I must admit we had not really asked ourselves that question. We are going to do so, and I believe the answers will be highly instructive - particularly in preparation for a meeting with the IT teams.

Beyond that, I make it a point to stay informed about global developments and evolving threats. I discuss this with our experts, who speak of a potentially paralyzing attack not as a remote possibility, but as something inevitable that we will face one day. As we say: it is not a question of “if,” but “when.”

In light of this, I fully agree with the report’s conclusions: **we cannot simply wait, we must prepare effectively. That is why I firmly believe that decisions and communications on these matters must be made at the Executive Committee level.** In other words, protecting our organizations on this front must be driven by the leadership team to ensure full mobilization across the company.

#2

Workshop

Ensuring Treasury operational continuity

Critical processes, Data availability & quality, Banking relationships

Ensuring Treasury operational continuity: critical processes, Data availability & quality, Banking relationships

The Taskforce's work highlights that Treasury Resilience in the event of a cyber crisis primarily depends on the Treasury team's ability to act autonomously and immediately.

Certain processes must be executable during a crisis, independently of other functions, in order to preserve the company's essential/important financial commitments. Among them, **salary payments** stand out as a top-priority vital process due to their direct social impact and strong internal visibility.

The Taskforce also emphasizes the importance of securing **critical suppliers payments** throughout the crisis, particularly in a context where supply chains are already fragile. Ensuring this continuity requires prior identification and prioritization, carried out in close coordination with procurement and business units, and based on a clear analysis of time-based impacts.

A shared prioritization framework is essential to enable rapid and consistent decision-making from the very early stages of the crisis.

Several other so-called **"Treasury" processes (debt servicing, settlement of market transactions, securitization)** may be perceived by senior management as more technical, yet they are no less critical to the company and its financing.

Finally, Treasury Resilience depends on the strength of **banking relationships** and the availability of **Vital Data**. The Taskforce highlights the need to integrate banking partners into the crisis management framework and to secure access to essential Treasury data within independent environments that remain usable in degraded mode. These elements are structural levers for maintaining operational capacity during the crisis and preparing for a controlled return to normal operations.

Workshop #2

Employees

→ Securing the payroll process

Salary payments are a central issue in times of crisis due to their immediate social impact and high internal visibility. In this context, the Taskforce emphasizes that the ability to execute payroll in a reliable and secure manner - including in degraded environments - is a key factor in maintaining stability and control during a crisis.

Securing the payroll process requires prior preparation, including the identification of critical dependencies (payroll data, approval workflows, banking relationships), as well as the definition of backup operating procedures. The ability to rely on recent reference data that has been secured and remains accessible, and to rapidly mobilize the relevant stakeholders, is essential to ensuring the continuity of the company's commitments to its employees.

Salary payments represent a highly visible issue within organizations and can become a decisive lever in raising awareness among senior management and business units about the need to invest in Treasury protection against cyber risk.

Critical suppliers

→ Preserving strategic relationships

Supplier relationships are profoundly affected by geopolitical tensions and sometimes abrupt supply chain disruptions, which alone can bring the entire production process to a halt. In this context, the Taskforce emphasizes that the ability to maintain supplier payments during a crisis is a decisive asset - both to limit immediate impacts and to accelerate the recovery phase.

Defining critical suppliers remains complex and cannot be standardized across the entire organization. This is why it is essential to establish in advance, together with business units, a clear and shared list of priorities: suppliers indispensable to operational continuity (for example: cloud platforms), vulnerable suppliers, and others.

This work must be updated regularly to avoid any ambiguity in decision-making during a crisis. Taxes and duties may, where relevant, also be included in the list of critical suppliers.

In a crisis, everything becomes critical to everyone. Therefore, defining a priority list requires a clear hierarchy of urgencies, linked to the timing and sequence of impacts on different stakeholders.

Treasury processes

→ Preserving financial capacity for action

Certain Treasury processes - beyond employee and critical supplier payments - form an essential foundation for the company's financial continuity (debt servicing, market operations, financial hedging, etc.). The Taskforce emphasizes that, in a crisis situation, their interruption can lead to immediate consequences in terms of liquidity, compliance with contractual obligations, and financial credibility with banking partners and the markets.

This requires defining in advance backup operating procedures that ensure the continuity of essential operations on Day 0 or Day 1, independently of the availability of usual management tools.

What is critically important during a cyber crisis is being able to maintain and update business and payment data, and then ensure that there is a clear and accurate record of what has been processed or paid through these secondary channels.

Banking relationships

→ Strategic partnership

The continuity of cash flows in a crisis situation depends above all on the ability to activate operational payment channels and on the quality of banking relationships.

In this regard, the Taskforce's work shows that the mere availability of Treasury Management Systems (TMS), even when hosted in the cloud, is not sufficient to guarantee Treasury's ability to act. In the event of a major cyber crisis, the unavailability of authentication systems or

approval mechanisms may render these tools inaccessible, even if they remain technically operational.

The implementation of complementary and independent arrangements is therefore essential to maintain a minimum capacity to act on critical cash flows.

In this context, several prerequisites appear essential:

- Proactively communicate the **crisis management plan** to the banks that may be required to step in
- Regularly test **backup web banking solutions** (where available)
- Clearly differentiate **payment banks and collection banks**
- Store **critical bank account details** in an independent, secure storage environment accessible in degraded mode, as exclusive reliance on paper-based records has shown operational limitations.

The key question remains whether crisis management should be entrusted entirely to a single bank or distributed among several partner banks. According to the Taskforce, relying on a single bank presents risks in terms of vulnerability and confidentiality and should therefore be avoided.

It is preferable to rely on a limited number of banking partners, selected in advance, trained in crisis management procedures, and with whom backup payment arrangements have been formally established.

Assessing the severity of a crisis

At the heart of managing a cyber crisis affecting Treasury is the need to establish a time-based severity scale: who is impacted, and who must be prioritized in the first hours, then the first days (and beyond), depending on the duration of the crisis?

In this context, the list of critical processes and suppliers primarily depends on the specific point in time at which they are affected. Similarly, the timing for activating a crisis action plan will depend on the urgency

of paying salaries, servicing debt, or supporting suppliers weakened by a payment disruption.

A rapid and reliable assessment of the crisis duration is a fundamental element of decision-making and directly determines the level of mobilization required from both internal and external stakeholders.

Maintaining access to critical Treasury Data

The definition of critical data stems directly from the work of identifying critical processes. The objective is not to retain all data, but to focus only on what is strictly necessary to maintain business continuity.

The identification of critical data must be based on collaborative work among stakeholders and then complemented by an assessment of data quality. This data must subsequently be exported to an independent, secure environment that ensures availability and confidentiality.

As this data is inherently dynamic, regular updates are essential. It is also necessary to identify a key contact for each critical process and ensure there is a reliable way to reach them under any circumstances.

Finally, maintaining operations during a crisis requires the ability to integrate newly generated data and to guarantee its compatibility and auditability when it is reintegrated into the information systems.

Astran expert view

The Taskforce's conclusions show that Treasury Resilience depends on the ability to operate in a degraded environment - and therefore on having access to vital processes and data.

This capability cannot rely on day-to-day management tools, even when they are hosted in the cloud, because in the event of a major crisis, nothing may be accessible to the Treasurer for several weeks. Ensuring availability during crises lies at the core of Astran's patented technology.

Protecting Treasury against a cyber crisis broadens the scope of action beyond the Treasury function alone to include accounts payable, procurement, and P2P functions, which are essential for identifying critical suppliers.

Treasury protection also helps drive a shift in internal culture—from a process compliance mindset to a genuine business protection mindset.

Salary payments are a major issue on which no compromise is acceptable.

Conclusion: getting started with a Treasury Resilience program

The Taskforce's findings outline key principles to successfully launch a Treasury Resilience initiative.

1. Assume total system outage

Consider that in the event of a major crisis (particularly of cyber origin), management tools, authentication systems, and usual access channels may be unavailable - including cloud-hosted software.

2. Prioritize a limited number of vital processes

Adopt a Minimum Vital Company (MVC) approach by focusing efforts on a restricted scope of processes that are essential to financial continuity, without attempting to cover all financial activities.

This prioritization must also take into account the regions, entities, or teams that are critical to executing these processes during a crisis.

3. Involve a limited number of stakeholders

From the outset, involve a small group of clearly identified participants: CISO, IT, Internal Control, Treasury, and, where appropriate, banking partners.

4. Start with one end-to-end process

Handle one initial process (simplified process, vital data, operational stakeholders) to demonstrate the value of the approach and create an initial, momentum-building success.

5. Test regularly through targeted crisis exercises

Implement regular, targeted crisis exercises with operational stakeholders to test the Resilience framework and institutionalize effective response behaviors.

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, synchronize, 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®

Keep critical processes running through disruption
Minimum Vital Company as-a-service

21 rue de Bruxelles
75009 PARIS

hello@astran.ai

www.astran.ai