StoneSight
Advisory Services

# DIVESTITURE

## Two businesses.
## Two futures.




Hundreds of decisions.
Consequences that outlast the transaction.

# A transaction can be on schedule. A business can still be unprepared.

A scheduled departure does not establish readiness. What appears straightforward from the passenger cabin depends on coordinated decisions, capable people, and systems working together. A divestiture presents executive leadership with the same challenge: knowing whether the organization is ready beneath the reassuring summary.

A divestiture can appear well controlled while consequential decisions accumulate beneath the executive dashboard. The transaction has owners, milestones, budgets, and workstreams. Yet across those workstreams, hundreds - sometimes thousands - of choices determine whether two independent businesses will emerge with the capabilities they need. Each choice may look reasonable in isolation. Together, they can create unnecessary expense, missing protection, conflicting responsibilities, and dependencies neither leadership team fully understands.

Having completed a divestiture before is valuable experience. It does not necessarily mean an executive has seen the entire separation. A finance leader may understand the economics without visibility into inherited security dependencies. A technology leader may deliver the migration without owning the contractual assumptions behind it. An operations leader may maintain continuity because another department quietly supplies capabilities that never appear in the operating plan. Familiarity with the transaction can conceal unfamiliarity with the exposure.

For the business being separated, independence offers an opportunity to build deliberately. For the divesting company, separation creates an obligation to reshape what remains. Both must sustain operations, protect information, retain essential knowledge, and meet financial expectations. Their objectives overlap, but their incentives can diverge. The parent wants to reduce cost and obligations. The separated business needs continuity and support. Decisions made to simplify one side can transfer complexity and risk to the other.

The separated business can modernize systems, simplify inherited arrangements, and establish clearer accountability. It can also spend an extraordinary amount of money before discovering that it has built the wrong capabilities. Vendors see a new customer. Implementation teams see deadlines. Executives want confidence that progress is being made. Purchased products and completed installations become reassuring evidence of activity. Whether they constitute the protection the business actually needs is a different question.

# Build what the business needs. Know what it depends on.

An ambition to build a highly mature security organization provides little direction by itself. Frameworks can organize requirements and expose gaps, but cannot decide which operational consequences the enterprise can tolerate or which investments deserve priority. Leadership must establish the intended business, its obligations, its dependencies, and its capacity to sustain the program. Without that foundation, a maturity target can become an expensive destination chosen before anyone agrees where the business needs to go.

A useful distinction separates **business operations critical** capabilities from **business critical** assets. The former keep the enterprise functioning: taking orders, producing goods, dispatching shipments, collecting cash, paying employees, and delivering services. Their loss can damage the company quickly. An inaccessible identity platform or corrupted production schedule may interrupt revenue before executives receive a complete explanation. The incoming CISO must understand these dependencies as business realities, including the less visible systems supporting them.

Business critical assets preserve value, competitive position, and obligations. Proprietary designs, customer information, pricing intelligence, research, and sensitive agreements may be compromised while operations continue apparently undisturbed. Damage can emerge gradually through lost advantage, weakened relationships, or contractual consequences. Some assets belong in both categories, and either kind of failure can unfold rapidly. This distinction helps leadership examine how harm develops; it does not justify postponing information protection until operations are stable.

The incoming CISO needs to begin with the business being created. What must work independently on day one? What must remain confidential, accurate, and recoverable? Which capabilities currently belong to the parent, and when will they disappear? Answers require engagement across Operations, Finance, Legal, Human Resources, and Technology. A CISO who begins with a preferred collection of products may build an impressive security function around an incomplete understanding of the company.

That incomplete understanding is particularly dangerous where protection has been inherited. A business unit may depend on the parent's identity systems, monitoring, recovery infrastructure, specialists, and vendor relationships without knowing their full contribution. A tool can transfer while its administrators remain behind. Data can migrate without a workable restoration process. A service can appear operational while responsibility for responding to an alert remains unresolved. Individual workstreams may report completion while the combined capability remains unfinished.



THE READINESS QUESTION

# A departure date is not evidence of readiness.

# The cost does not disappear because the business does.

This is where experienced judgment earns its value. Someone must look across the handoffs and ask what the completion reports fail to establish. Who will operate the capability? Who will respond when it fails? What supports the assumption that a supplier or former parent will act? A separation plan needs people who recognize these questions before an incident makes them obvious. Costly omissions are often familiar to those who have encountered them before.

Spending decisions deserve the same challenge. Every significant investment should connect to a business consequence, an accountable owner, and a way to demonstrate effectiveness. Costs extend beyond purchase price into integration, staffing, licensing, maintenance, and administration. An organization can overinvest in overlapping capabilities while leaving a critical dependency underfunded. Once contracts are signed and architectures established, correcting those decisions becomes harder. Experienced guidance helps leadership distinguish urgent requirements from expensive momentum.

Transition service agreements can create a reassuring impression of continuity. Their value depends on the services actually provided, their boundaries, and the conditions for withdrawal. Leadership needs clarity about access, incident coordination, service responsibilities, and replacement readiness. An approaching expiration date does not establish that the separated business can operate safely without support. Equally, repeatedly extending support can conceal a build that has lost direction. Both outcomes carry costs beyond the agreement itself.

The parent faces its own difficult adjustment. A smaller enterprise does not automatically produce a proportionately smaller security budget. Fixed contracts remain, shared platforms may still be required, and teams may support both businesses during transition. Allocated costs can leave the financial model while actual expenditure stays behind. Unless leadership distinguishes temporary costs, stranded costs, and sustainable requirements, expected savings may prove substantially harder to achieve than the transaction case suggested.

People decisions compound that challenge. If too few employees transfer, the parent may retain capacity its future workload cannot support. Growth, redeployment, or attrition may absorb some of it; otherwise, reductions may become necessary. Yet cutting by percentage can remove precisely the knowledge the retained enterprise needs. Both companies must understand which capabilities follow particular individuals, what must be transferred, and what coverage remains. A headcount allocation is not an operating model.

# Who sees the decisions between the workstreams?

These choices affect the incoming organization's ability to absorb what it receives. Transferred employees may inherit broader responsibilities, unfamiliar systems, or expectations previously distributed across a larger team. Retained employees may lose colleagues who supplied essential expertise. Neither condition is necessarily visible in a staffing total. Leadership needs a credible account of who will perform the work after separation, with what knowledge, and under what demands. Apparent efficiency can become dependence on a few exhausted people.

Executive leadership must bring these decisions together. Security cannot independently determine acceptable interruption, capital allocation, staffing commitments, or contractual exposure. Nor should its conclusions disappear inside another workstream's delivery priorities. A common decision process must expose tradeoffs, resolve conflicting assumptions, and identify who accepts unresolved risk. Boards may ask whether enterprise value and readiness are adequately protected. Management must answer with evidence extending beyond a green status report.

At StoneSight, our perspective comes from having navigated these separations and made difficult operating, technology, and security decisions within them. We understand the pressure to maintain progress, release resources, satisfy financial commitments, and build capabilities while the organization itself is changing. That experience informs our judgment about what deserves attention, where assumptions warrant challenge, and which apparent shortcuts create lasting obligations. We help executives see across departmental boundaries that transaction reporting can leave intact.

StoneSight provides experienced, independent judgment where decisions become commitments. We help leadership examine the business being built and the business being retained, connecting protection, staffing, spending, and transition readiness. Even capable executives benefit from someone who has seen how adjacent decisions interact. Before the next purchase, transfer, deadline, or cost reduction becomes difficult to reverse, the question is whether anyone has examined its full consequence. That is the perspective StoneSight brings to your next decision.

**A headcount allocation is not an operating model.**



STONESIGHT

ADVISORY SERVICES

# Build independence. Preserve value.

Experienced judgment for both sides of your next divestiture.

---

**advisory@stonesightadvisory.com**

stonesightadvisory.com

© 2026 StoneSight Advisory Services, LLC.