Know What You Own. Protect What Matters.

A practical executive guide to asset visibility, smarter technology spending, operational resilience, and business risk management.

Most executives know what their company spends on technology. Far fewer can confidently say they have a reliable, continuously maintained view of the applications, systems, data, connected equipment, and external services their business depends on.

That gap can be expensive. You may be paying for technology nobody uses, maintaining equipment nobody owns, or relying on critical systems that lack appropriate protection and recovery capabilities.

Imagine knowing what is in use, what it costs, who owns it, and how it keeps your business operating. You can uncover waste, understand critical dependencies, direct investment where it matters, and show leadership that important risks are being managed.

The outcome: greater control, smarter spending, operational resilience, and confidence backed by evidence.

Your five-phase action plan

Phase	What you do	What you gain
01 Gather	Discover applications, infrastructure, data, cloud, connected equipment, OT, IoT, and external services.	Know what exists.
02 Organize & map	Reconcile records, assign owners, and document dependencies and data flows.	Understand how it connects.
03 Assess & prioritize	Use a BIA to define business criticality, protection needs, and recovery priorities.	Know what matters most.
04 Identify gaps	Review spending, lifecycle, cybersecurity, recovery, compliance, and accountability.	Find waste and exposure.
05 Remediate & manage	Address gaps and establish continuing discovery, maintenance, and oversight.	Maintain visibility and control.

What success looks like

A trusted asset register tied to business operations; confirmed owners and dependencies; protection and recovery priorities; a prioritized improvement roadmap; and evidence that the information stays current.

Most organizations already have pieces of this information across tools, contracts, spreadsheets, vendors, and employees. The work is to bring it together, verify it, identify what is missing, and keep it accurate.

Complete visibility is the destination. Prioritization is how you get there. Ongoing management is how you stay there.

Begin with the most critical systems and operations, then expand methodically. The practical target is **comprehensive, verified visibility across your defined environment**, supported by continuing discovery as the business changes.

The following pages show how to accomplish each phase, what your team must do, and what it should deliver.

Better visibility creates better business decisions.

Every business depends on technology, data, equipment, and outside services. Some assets are obvious; others quietly support essential functions without appearing in a current inventory.

Money gets wasted. Unused subscriptions renew, departments buy overlapping software, and maintenance continues for assets no longer delivering value.

Operations become harder to manage. An aging system cannot be replaced confidently because its dependencies are unclear; a minor integration turns out to support a major process.

Cybersecurity gaps go unnoticed. Unknown devices, unmanaged applications, forgotten data repositories, and connected equipment can fall outside appropriate oversight.

Recovery becomes more complicated. A server is restored but the business process still fails because a database, cloud integration, or external provider remains unavailable.

Executive visibility check: five questions worth asking

1. Do we know what technology and data our business depends on? Include cloud, outside providers, connected equipment, and departmental applications.

2. Do we know who owns our most important assets? Confirm both the technical owner and the business decision-maker.

3. Do we understand critical dependencies? Know what else must work to restore a business operation.

4. Can we identify wasted spending and unmanaged exposure? Consider unused software, unsupported technology, and unverified security coverage.

5. Can we show that our critical assets are appropriately managed? Look for evidence of protection, recovery, ownership, and investment decisions.

If any answer is uncertain, you've identified a place to start.

Ask IT, operations, and security leaders to review the questions together. For every uncertain answer, note **what is missing, who will validate it, and whether a critical business operation is affected**. Address the most important dependencies first, then work systematically toward reliable coverage across the environment.

What this means for leadership

Role	Value delivered
CEO	Confidence in critical dependencies, accountability, and business risk decisions.
COO	Fewer operational surprises and clearer continuity and recovery priorities.
CFO	Better spending visibility, less avoidable waste, and defensible investment.
CIO / IT leader	Reliable records, clear ownership, and a practical technology roadmap.
CISO	Better visibility into what needs protection and evidence of control coverage.



Discover what your business actually uses.

Objective: Build an inventory of the technology, applications, data, connected equipment, and external services supporting the organization. Existing records are a starting point, not proof of completeness.

1. Collect what you already know

- IT inventories, CMDBs, network discovery, monitoring, and architecture records.
- Procurement, invoices, software licensing, contracts, and renewal lists.
- Cloud consoles, SaaS administration, hosting, security tools, and backups.
- Application documentation, vendor records, and existing network or data-flow maps.

Record the source, date, and confidence level of information. Conflicting records need investigation rather than guesswork.

2. Interview the people who run the business

Automated tools cannot explain every undocumented business relationship. Interview business and process owners, operations, IT, security, finance, facilities, and relevant vendors.

• What systems, equipment, applications, and information does your team rely on?

• What would happen if those resources became unavailable or inaccurate?

• What data do you create, store, process, or share, and with whom?

• Which departments, vendors, and integrations do you depend on?

• Who owns, maintains, pays for, and authorizes changes to these assets?

• What has been added, replaced, moved, or retired recently?

Look for departmental software purchases, custom applications, undocumented connections, and assets known only to one employee.

3. Validate with appropriate technical discovery

Compare interviews and existing records with asset discoveries across on-premises, remote, cloud, OT, and IoT environments. Consider industrial controllers, scanners, sensors, telematics, and other connected equipment. **Use methods appropriate to sensitive OT and operational environments; passive or nonintrusive discovery may be necessary.**

Important data repositories need their own review: finding a device does not establish what information it holds or how that information moves.

4. Reconcile the results

Investigate duplicates, unknown assets, outdated records, and inconsistent ownership. Assign unresolved findings for follow-up instead of silently removing uncertain entries.

Deliverable: Consolidated initial inventory, sources, verification status, and discovery exceptions.

Process / department	Environment	Existing information source	Person interviewed	Technical evidence	Owner candidate	Verification status	C
Dispatch	Hybrid	IT application list	Dispatch Manager	Application inventory	Operations Director	Verified	R
Shipment dispatch	Primary data center	VM inventory	IT Director	Hypervisor discovery	Infrastructure Lead	Verified	C
Shipment dispatch	Primary data center	DB administration	Applications Lead	DB inventory	Database Administrator	Verified	C
Shipment dispatch	Primary data center	DB administration	Dispatch Manager	DB inventory	Database Administrator	Verified	V
Authentication	Cloud / on-prem	IAM console	IT Director	Identity discovery	IT Director	Verified	C
Dispatch / tracking	Third party	Partner contract	Operations Lead	SaaS/API review	Unassigned	Needs review	F
Shipment tracking	Cloud provider	SaaS billing	Client Service Lead	SaaS admin console	Operations Manager	Verified	V
Warehouse labeling	Warehouse	Network scan	Warehouse Manager	Passive discovery	Warehouse Manager	Needs review	R
[illegible]heduling	Cloud provider	Credit card expense	Finance Manager	SaaS subscription export	HR Director	Needs review	U
		Operations register	Warehouse Manager	Passive discovery			

An inventory tells you what exists. Context tells you why it matters.

A device inventory may identify a server or database. It will not necessarily tell leadership which revenue-generating activity depends on it, what it costs, or who can authorize a change. **Good asset management connects technical visibility with business purpose, cost, ownership, and risk.**

1. Build an asset register that supports decisions

Record	Include
Identity	Asset ID, name, category, location.
Accountability	Business owner, technical owner, responsible team.
Business purpose	Processes supported, users, services delivered.
Financial & lifecycle	Costs, contracts, renewal, support and retirement status.
Relationships	Applications, infrastructure, service providers, integrations.
Data & management	Important datasets, data flows, security, backup and verification status.

Use a CMDB, asset management platform, or structured spreadsheet. Business criticality and risk ratings can be refined after the BIA.

2. Map dependencies and data flows

Consider a transportation management system (TMS) running on **Server A**. It might also require an operational database, a separate shipment database, an identity service, a cloud API, a carrier or EDI partner, and synchronized information.

Restoring Server A doesn't necessarily restore shipment dispatch.

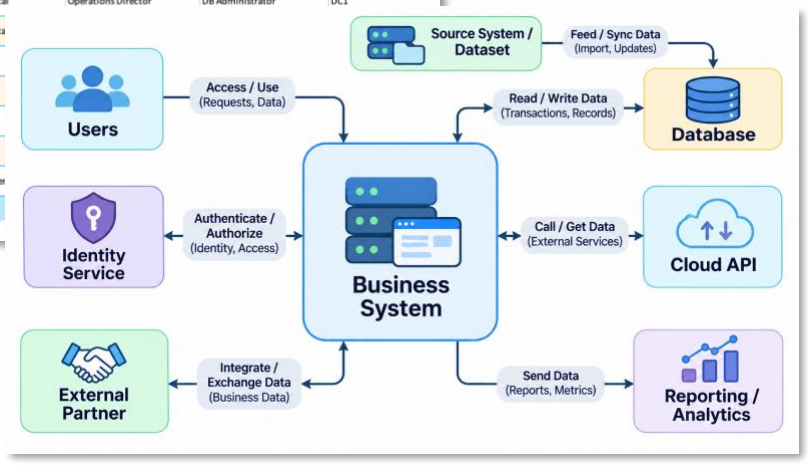
The server may be available while the cloud interface is down, a partner connection is unavailable, or the databases are inconsistent. For important processes, identify **what each asset depends on and what depends on it**. Document where critical data originates, travels, is stored, and is accessed.

3. Validate with the business

Technical teams can map connections; business owners validate operational purpose, actual workarounds, responsibility, and consequences. Record unknown dependencies and assign someone to resolve them.

Deliverable: Asset register, confirmed ownership, business context, and initial dependency and data-flow maps.

Asset / System	Category	Business process	Department	Criticality	Business owner	Technical owner	Hosting / location
TMS Application	Application	Shipment dispatch	Operations	Critical	Operations Director	Applications Lead	Hybrid / DC1
TMS App Server A	Server	Shipment dispatch	IT	Critical	Operations Director	Infrastructure Lead	DC1 / VM
Operations DB	Database	Shipment dispatch	IT	Critical	Operations Director	DB Administrator	DC1
Customer & Shipment DB	Database	Shipment dispatch	IT	Critical	Operations Director	DB Administrator	DC1
Identity Service	Identity	Dispatch authentication	IT	Critica			
Carrier EDI / API	Integration	Shipment dispatch	Operations	High			
Cloud Shipment Tracking	Cloud/SaaS	Shipment tracking	Operations	High			
Legacy Label Gateway	OT/IoT	Warehouse labeling	Warehouse	High			
Scheduling SaaS	SaaS	Staff scheduling	HR	Low			
		Warehouse receiving	Warehouse	Moder			



Protect what matters. Recover what matters first.

Not every asset has equal importance. Use a **Business Impact Analysis (BIA)** to understand the consequences of disruption or compromise, then connect those impacts to the applications, data, infrastructure, and suppliers identified in earlier phases.

1. Evaluate business consequences

Interview process owners about operational disruption, revenue and added costs, client commitments, sensitive information, safety, compliance, reputation, and the effects of inaccurate data. Examine how impact changes after four hours, one day, or several days; choose intervals that fit the business.

2. Set business-based priorities

Rating	Meaning
Critical	Loss or compromise creates unacceptable impact on essential operations, safety, obligations or viability.
High	Serious disruption or exposure requiring prompt response.
Moderate	Manageable impact with defined alternatives or workarounds.
Low	Limited financial, operational or regulatory consequences.

Use organization-specific impact criteria. The most technically complex system is not always the most important to the business.

3. Define protection and recovery requirements

- **Protection:** Appropriate access, monitoring, maintenance, integrity, confidentiality, and availability safeguards.
- **Recovery Time Objective (RTO):** How quickly the process or system must be restored.
- **Recovery Point Objective (RPO):** How much data loss, measured in time, the business can tolerate.
- **Recovery sequence:** The prerequisites that must be working before the business process can resume.

Server A could be a visible recovery priority, but the database, identity provider, integration, or partner connection might need to recover first. Verify recovery order against the actual dependency map.

4. Apply business risk appetite and obligations

Leadership defines acceptable residual risk and approves tradeoffs. Legal, regulatory, safety, and contractual requirements set obligations that cannot simply be waived. Other decisions balance impact, cost, protection, and tolerance.

Deliverable: BIA, priority ratings, protection needs, recovery objectives and a validated recovery sequence.

Business process	Process owner	Impact if down 4h	Impact if down 24h	Impact if down 72h	Priority
Shipment dispatch / load management	Operations Director	Dispatch delays; manual workarounds	Missed pickups / contractual exposure	Sustained interruption; major escalation	Critical
Customer shipment tracking	Operations Manager	Stale tracking updates	Client escalations and staffing expense	Contract impacts and trust erosion	High
Warehouse labeling & receiving	Warehouse Manager	Manual labels / slower receiving	Throughput loss and rework	Sustained delivery backlog	High
Client invoicing	Finance Director	Invoice delays	Cash collection may be delayed	Month-end processing disruption	Moderate
Staff scheduling	HR Director	Minor scheduling workarounds	Manual roster maintenance	Administrative inefficiency	Low

Find the waste. Understand the exposure.

Compare what your business needs with the actual condition and management of its assets. This is where visibility becomes useful for financial, operational, cybersecurity, and governance decisions.

Area	What to review
Visibility & ownership	Unknown or duplicated assets, stale records, missing accountable owners.
Dependencies & data	Unverified integrations, flows, suppliers and repositories.
Spending & lifecycle	Unused licenses, duplicated tools, renewals, obsolete or unsupported systems.
Cybersecurity	Coverage, access controls, monitoring, patching and vulnerability management.
Recovery	Backup scope, restoration testing, RTO/RPO feasibility and process recovery.
Compliance & governance	Applicable obligations, policies, approved decisions and recorded risk acceptance.

What a visibility gap can mean financially

Consider several departments purchasing software independently. Without reliable usage, ownership, and contract records, subscriptions may renew for redundant applications or licenses that nobody needs. Reliable asset visibility enables informed consolidation and retirement decisions.

The same principle applies to risk. **A critical application may have a relatively modest annual operating cost, yet its failure could disrupt operations, delay revenue-generating activities, or create significant financial consequences.**

Without understanding its dependencies or recovery requirements, leadership cannot reliably evaluate whether the current investment in protection is appropriate.

The goal isn't simply to spend less. It's to spend where technology creates value and where protection matches business need.

Record findings that can be acted upon

- Affected asset and the business operation it supports.
- Gap, supporting evidence and potential business consequence.
- Recommended response, accountable owner and target date.
- Priority, cost or effort estimate, and decision or approval status.

Connect material risk findings to the risk register. Avoid turning unsupported assumptions into formal findings.

Deliverable: Evidence-based gap register, cost optimization opportunities and prioritized risk findings.

Business process	Category	Gap / supporting evidence	Potential business impact	Priority	Risk treatment	Accountable owner
Shipment dispatch	Ownership / third party	Carrier EDI/API escalation owner not confirmed	Delayed partner recovery and incident coordination	High	Reduce	Operations Director
Warehouse labeling	Lifecycle / OT	Connected label gateway has no current vendor support	Operational disruption and unmanaged exposure	High	Reduce	Warehouse Manager
Shipment dispatch	Recovery / data	End-to-end shipment database recovery not tested	Recovery of server may not restore dispatch	High	Reduce	IT Director
Staff scheduling	Spend / licensing	Unused subscription duplicates approved scheduling tool	Unnecessary recurring expenditure	Low	Eliminate	Finance Director
Shipment tracking	Spend / cloud	Cloud service has potentially unused seats	Potential recurring waste	Moderate	Optimize	Operations Manager
Shipment dispatch	Governance	After-hours escalation responsibility updated	Previously unclear notification handoff	Moderate	Reduce	CISO
Shipment dispatch	Security	Database security monitoring scope incomplete	Potential undetected exposure on a critical system	High	Reduce	Security Lead

Turn visibility into action and better decisions.

Understanding gaps creates opportunity. Addressing the right ones creates value. Turn findings into an improvement roadmap that reflects business consequences, obligations, effort, and executive priorities.

Choose the right response

Eliminate unnecessary assets. Retire unused applications and services, remove unauthorized technology safely, and stop avoidable expenses.

Optimize investments. Consolidate overlapping platforms, improve licensing, renegotiate contracts, and plan lifecycle replacements.

Improve protection. Close relevant security, access, monitoring, maintenance, and vulnerability-management gaps.

Strengthen resilience. Improve backups, dependencies, tested recovery, failover and process-level restoration.

Accept or transfer appropriate risk. Document justified risk acceptance by authorized leaders, or transfer defined financial consequences through contracts or insurance. Risk transfer does not remove operational responsibility.

Prioritize, fund, and assign the work

Evaluate actions by **business impact**, **urgency** (including mandatory obligations and unacceptable risk), and **effort or investment**. Prioritize material improvements while coordinating changes that affect critical operations.

Do not remove technology solely because it appears obsolete. Validate dependencies and data-retention requirements before changes.

Verify outcomes rather than ticket closure

Every action should have an owner, outcome, target date, and evidence of completion. Replacing an unsupported server, for example, is only successful when the dependent applications, data, integrations, and business processes continue working.

Deliverable: Approved improvement roadmap, owners, investment decisions, and evidence of completed remediation.

Phase	Action / task	Related finding	Accountable owner	Priority	Est. one-time cost ($)	Expected business outcome	Target da
Gather	Reconcile discovery sources and initial asset IDs		IT Director	High	-	Reliable baseline	
Organize & map	Confirm carrier EDI/API owner and recovery playbook	GAP-001	Operations Director	High	$2,500	Clear third-party escalation	
Assess & prioritize	Test full shipment DB and TMS recovery	GAP-003	IT Director	Critical	$5,000	Evidence of end-to-end dispatch recovery	
Remediate	Replace unsupported warehouse label gateway	GAP-002	Warehouse Manager	High	$11,000	Restore vendor support and limit exposure	
Remediate	Retire redundant scheduling subscription safely	GAP-004	Finance Director	Moderate	-	Avoid $6,000 illustrative annual cost	
Manage	Implement quarterly business-owner attestations		Program Owner	Moderate	-	Keep records and owners current	
Remediate	Extend security monitoring to critical operations DB	GAP-007	Security Lead	High	$4,000	Improve coverage for critical data service	
Manage	Establish continuous reconciliation into CMDB		IT Director	Moderate	$3,500	Reduce unknown/stale asset records	

Keep visibility current as the business changes.

The value of asset visibility isn't measured by how accurate your inventory was on the day it was completed. It's measured by whether leadership can continue relying on that information as the business changes.

People join and leave. Departments buy tools, cloud environments expand, vendors change, and technology is replaced. Asset management must therefore operate as an ongoing business capability, not a one-time inventory project.

Make lifecycle management routine

- **Onboard:** Capture new applications, infrastructure, data repositories, connected devices and services.
- **Change:** Update owners, configuration, location, dependencies, criticality and data flows.
- **Reconcile:** Compare asset records to regular discovery, procurement and administration records.
- **Review:** Track support status, renewal, warranty, cost, protection and risk requirements.
- **Retire:** Validate dependencies, handle data appropriately, remove access and terminate unused spending.

What an executive dashboard can show

Leadership measure	Illustrative result
Known assets verified during the reporting period	92%
Critical assets with accountable business owners	87%
Unresolved critical dependencies	14
Open high-priority management / protection gaps	8
Validated technology cost optimization opportunities	6

Illustrative values only, not viLogics client results. "Known assets verified" uses the known-asset population for the defined reporting period, not an assumed count of every asset in the environment. Report discovery coverage separately by environment and method; show unresolved scope and blind spots.

Priority actions: Confirm critical dependencies (IT/Operations); review redundant software (IT/Finance); validate recovery coverage (IT/Security).

Assign continuing accountability

IT maintains technical records; process owners confirm purpose and accountability; finance supports spending visibility; security evaluates exposure; operations validates dependencies; leadership approves material risk and investment decisions.

Deliverable: An operating model with validated records, recurring discovery, leadership reporting and accountable action.

Your asset visibility implementation playbook.

Goal: Comprehensive, verified visibility across the defined environment. Start with critical operations, then expand in planned waves until all relevant business units, technologies, data and connected assets have been assessed. Track exceptions rather than quietly treating undiscovered assets as covered.

Phase / lead	Core activities	Deliverable
1 Gather IT / Asset management	Name sponsor and owner; define scope; collect records; interview teams; discover and reconcile assets.	Consolidated inventory, source records, exceptions.
2 Organize & map IT + business owners	Define categories; assign owners; map processes, data flows, integrations, providers and dependencies.	Asset register, ownership and relationship maps.
3 Assess & prioritize Business / Ops + IT + Security	Run BIA; confirm impact and obligations; rate criticality; define protection, RTO/RPO and recovery order.	BIA, priority ratings, protection and recovery needs.
4 Identify gaps IT + Security + Finance	Review inventory, spending, lifecycle, protection, backups, obligations and decisions; capture evidence.	Gap/risk register and cost opportunities.
5 Remediate & manage Program owner + executives	Approve investment; assign actions; verify results; set onboarding, retirement, discovery and reporting cadence.	Roadmap, risk decisions and ongoing management model.

Five working documents

- **Asset register:** What exists, its owner, purpose, cost and lifecycle.
- **Dependency / data-flow map:** How processes, systems, data and external services connect.
- **Business Impact Analysis:** Which processes and assets matter and required recovery targets.
- **Gaps and risk register:** What is missing, business implications and recommended treatment or decisions to accept.
- **Improvement roadmap:** Owners, budgets, actions, milestones and evidence of completion.

Companion download

Asset Visibility Implementation Workbook: Five editable worksheets, with sample entries and instructions, to help teams inventory assets, map dependencies, assess business impact, document gaps and plan improvements.

[WORKBOOK DOWNLOAD LINK]

What completion means: Defined and evidenced coverage; accountable owners for critical assets; validated dependencies; documented priorities and gaps; and a process to keep information current. The duration depends on organizational complexity and existing records.

Methodology note: This five-phase approach is viLogics' practical adaptation of established principles from NIST CSF 2.0 (ID.AM), NIST IR 8286D (BIA and risk prioritization), CIS Controls v8.1 (asset/software inventories), and ISO/IEC 19770-1 (IT asset management). It is not presented as a formal sequence prescribed by those frameworks.

The playbook is yours. The work doesn't have to be.

This guide gives you the methodology and project plan to build an asset visibility and management program internally. You know what to discover, how to organize it, how to understand dependencies and business impact, and how to turn findings into better decisions.

For many organizations, the challenge is finding the time, skills, and capacity to complete the work thoroughly while keeping everyday operations running. **That is where viLogics can help.**

The same five phases, delivered with experienced people and technology

Phase	How viLogics can help
Gather	Stakeholder interviews, asset discovery and inventory reconciliation.
Organize & map	Asset register, CMDB support, ownership, dependencies and data flows.
Assess & prioritize	BIA facilitation, business criticality, protection and recovery priorities.
Identify gaps	Exposure assessment, lifecycle review, spend optimization and risk findings.
Remediate & manage	Improvement plan, remediation coordination, recurring visibility and reporting.

Technology supports the process; people make the decisions

viLogics can use **Armis from ServiceNow** to identify connected assets and cyber exposures across supported IT, OT, IoT and cloud environments. Where the relevant integrations and licenses are in place, asset intelligence can contribute to a **ServiceNow CMDB** and support IT, cybersecurity, and risk-management workflows.



A discovery tool can identify an asset. It cannot decide for the business what that asset is worth, what risk is acceptable, or who must approve a response. We connect technical evidence to business context, ownership and action.

Choose how much to own and how much to delegate

Some organizations need a reliable baseline. Others have inventories but want deeper dependency mapping, a better BIA, support maintaining the CMDB or risk register, or ongoing exposure and lifecycle management. viLogics can establish the program, work alongside your team, or take on defined parts of continuous operations.

Your leadership team retains the business decisions. We provide the expertise, repeatable process and technology needed to help carry out the work.

Know what you have. Know what matters. Know it is being managed.

Reliable asset visibility helps leadership make better decisions about technology investment, operations, cybersecurity and business risk. Whether you are establishing the foundation, improving an existing program, or looking for a partner to maintain it, viLogics can help.

The playbook is yours. The work doesn't have to be. Start the conversation >> with an asset management advisor now.