Timly

Cybersecurity Asset Management & Compliance

A Centralized Asset Register for Reduced Risk and Audit Readiness

Photo Courtesy

Table of Contents

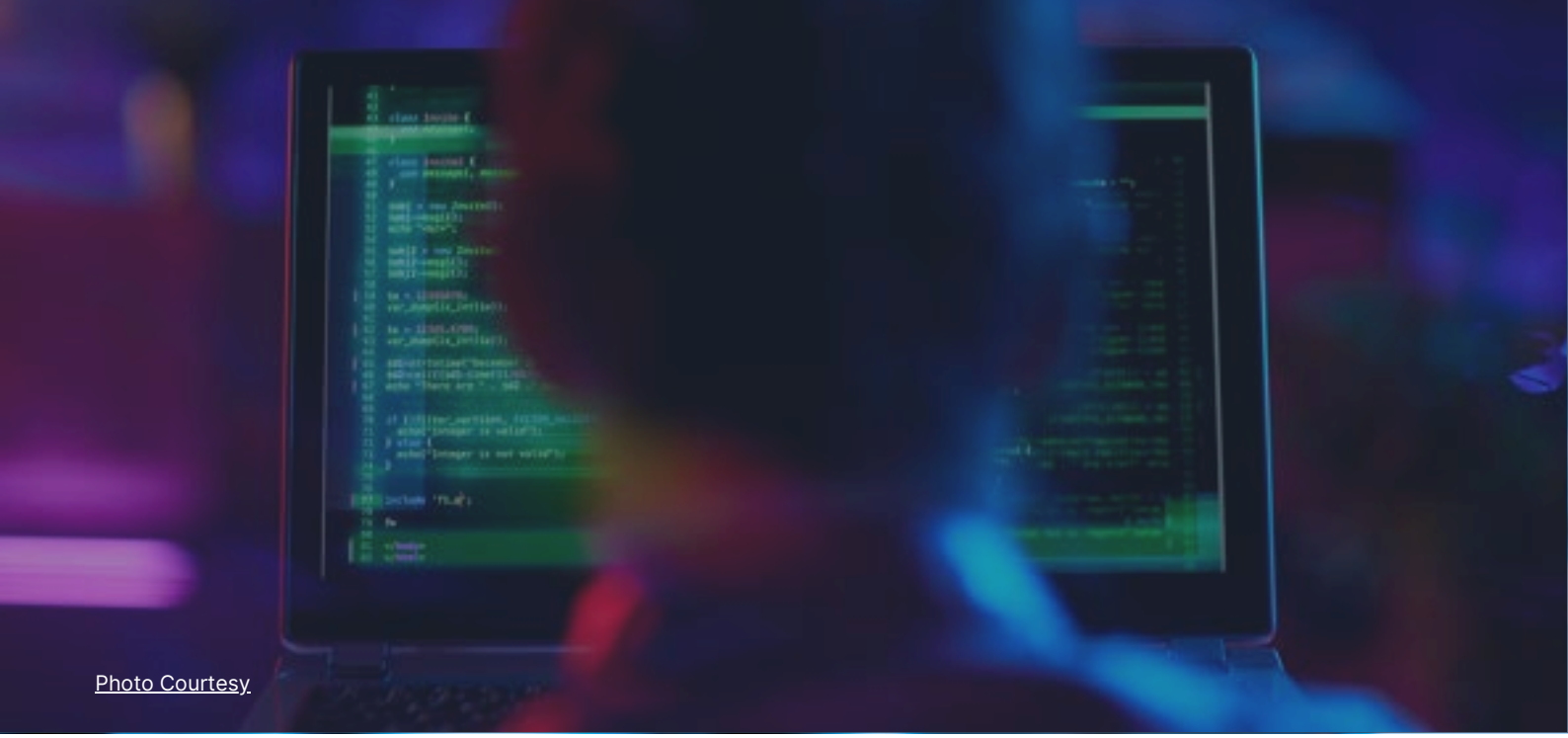


Photo Courtesy

Foreword & Objectives of This Report

You can't protect assets if you don't know where they are. Yet, this is the reality in many companies today: inventories exist, but they are fragmented, outdated, or lack sufficient security.

The result is blind spots, delayed incident response, and compliance evidence that must be gathered manually. This report explains why a centralized asset register is the operational foundation of effective cybersecurity—and how organizations can build and maintain one in practice.

1.1 Why Cybersecurity Asset Management Is a Top Priority Now

Organizations' attack surfaces are expanding faster than many security and operating models can keep up with. In addition to traditional IT assets such as laptops, servers, and network components, today's security landscape also includes cloud resources, SaaS applications, identities, third-party service providers, IoT components, and connected OT systems.

This is particularly true in industries such as IT, construction, manufacturing, facility management, and technical services, where highly dynamic environments are created through changing locations, mobile devices, temporary infrastructure, and shared responsibilities among IT, operations, and other business units.

The core challenge is rarely a lack of technology. Many organizations already maintain separate inventories, CMDBs, network scans, cloud portals, or endpoint tools. Yet key questions often remain unanswered: **Which security-relevant assets actually exist? Who owns them? How critical are they? And what is their current security posture?**

This gap transforms ordinary inventory management into a critical cybersecurity issue, and its importance is measurable.

- According to Verizon's "Data Breach Investigations Report 2025", 46% of compromised systems with potential corporate login credentials in one analyzed dataset were **not integrated into the organization's centralized management environment.**[1]

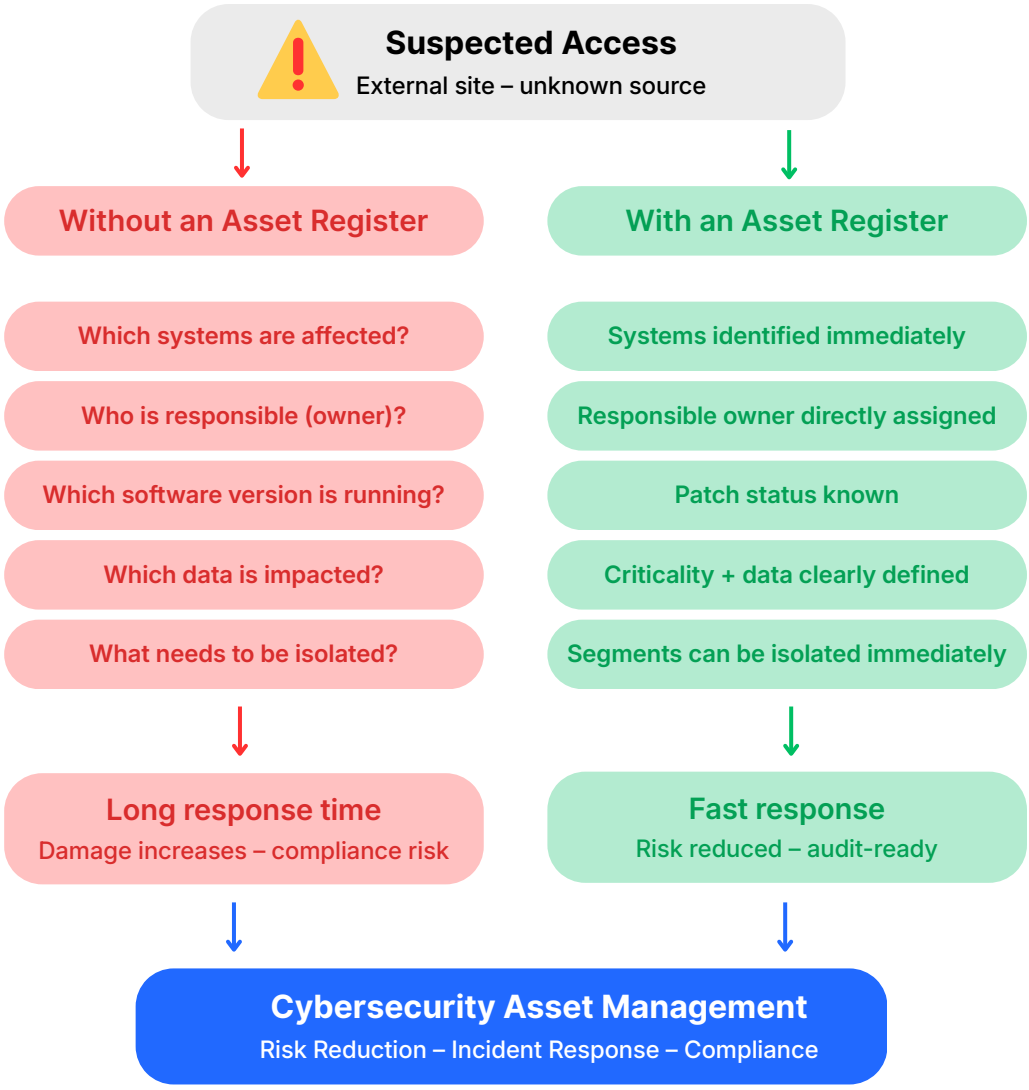
- IBM's "Cost of a Data Breach Report 2025" also found that 40% of analyzed breaches involved data across multiple environments, and those incidents required an average of 283 days to identify and contain.[2]

A simple example illustrates the importance of visibility: a suspicious access attempt, whether through an external system or a poorly maintained cloud account, immediately highlights how critical transparency across all assets is.

Without a centralized asset view, incident response teams lack clear answers to questions such as: Which systems are affected? Who is responsible? What data is involved? What needs to be isolated? This delays response efforts and increases risk.

By contrast, a robust asset register enables affected systems to be identified immediately, prioritized appropriately, and assigned to responsible stakeholders. The following illustration demonstrates how information such as patch status, criticality, network segments, identities, interfaces, and locations can be made centrally available, enabling rapid, audit-ready response capabilities.

Cybersecurity Asset Management therefore evolves from a niche inventory discipline into a prerequisite for effective risk reduction, operational incident response, and sustainable compliance.



1.2 Who This Report Is For

This report is **intended for organizations seeking to build their security and compliance processes on a reliable asset foundation.**

It is particularly relevant for:

- CISOs and information security leaders
- IT management and IT operations teams
- OT and production managers
- Facility management leaders
- Compliance, risk, and audit professionals
- Internal audit and governance teams

Many organizations are already familiar with foundational security standards and regulatory requirements, such as ISO 27001, NIS2, or industry-specific frameworks. **What is often missing, however, is a practical approach for building and maintaining a complete and secure asset inventory in day-to-day operations.**

This is where the report provides guidance. It combines technical, organizational, and process-oriented perspectives and demonstrates how organizations can establish a centralized asset register as the foundation of their security strategy.

1.3 Objectives & Structure of This Report

This report demonstrates why an incomplete asset inventory is not merely an administrative issue, but a **direct cybersecurity and compliance risk**. It explains how unknown assets, unclear ownership, and fragmented asset data weaken patch management, incident response, audit readiness, and management reporting.

Building on this foundation, the report outlines the **requirements for a robust asset register imposed by standards and regulatory frameworks**. It also provides a practical target-state model for building a secure asset register, including: relevant asset classes, roles and responsibilities, a simple maturity model, core security processes, and sample KPIs.

The report further develops a 90-day blueprint that organizations can use to assess their current maturity level and prioritize concrete improvements.

Photo Courtesy

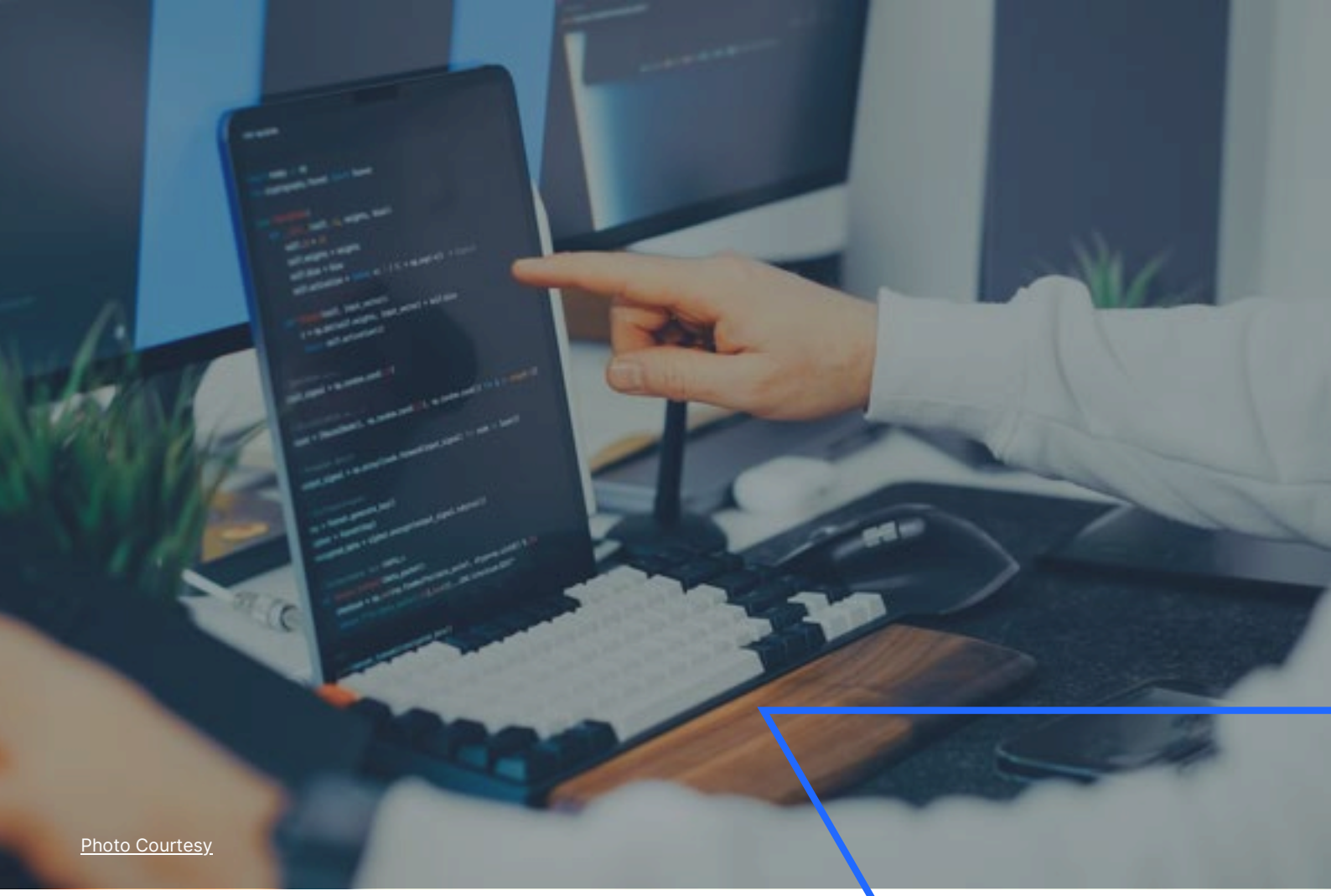


Photo Courtesy

What is Cybersecurity Asset Management (CSAM)?

Definitions & Scope

What is Cybersecurity Asset Management (CSAM)?
Definitions & Scope

Before building an asset register, organizations need a clear understanding of one fundamental question: What exactly falls within the scope of Cybersecurity Asset Management, and how does it differ from traditional IT Asset Management?

2.1 Definition & Differentiation

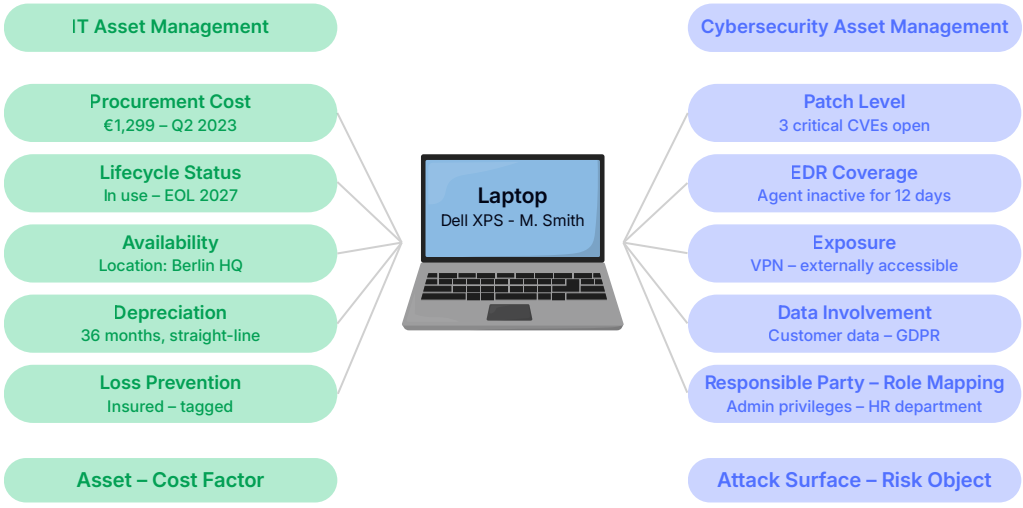
Before building an asset register, organizations need a clear understanding of one fundamental question: What exactly falls within the scope of Cybersecurity Asset Management, and how does it differ from traditional IT Asset Management?

Unlike traditional IT Asset Management, the primary focus is not on operational or financial lifecycle management. Instead, the focus is on understanding the risks, dependencies, and attack surfaces associated with each asset.

While **ITAM primarily views assets as operational or cost-related objects, CSAM extends this perspective by incorporating security and compliance context**, including patch status, exposure level, criticality, identities, vulnerabilities, ownership and accountability.

As a result, **a managed device becomes a managed security object**.

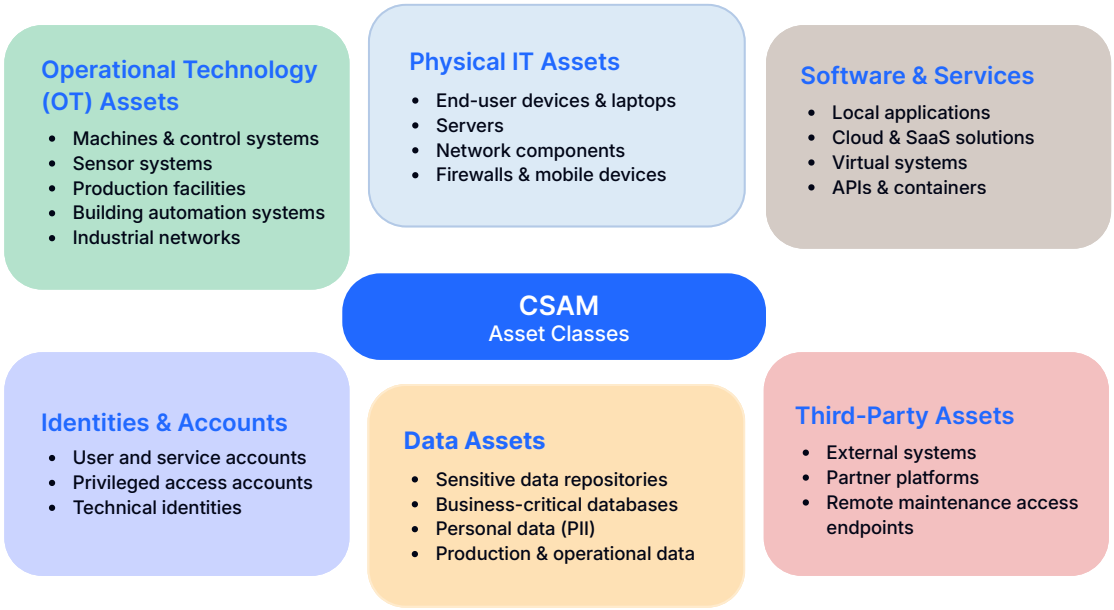
The following illustration highlights this shift in perspective through a practical example. While a laptop in an ITAM context is primarily viewed as a managed operational device, in a CSAM context the emphasis is placed on its security and risk profile, including ownership, patch status, exposure level, and implemented security controls.



2.2 Which Asset Classes Are Included in Scope?

Effective Cybersecurity Asset Management encompasses far more than traditional endpoints and servers. In principle, all items capable of creating security, compliance, or operational risks should be included.

Typical Asset Classes in CSAM:



The key factor is not merely the existence of an asset, but its context:

- Criticality
- Ownership
- Security status
- Dependencies
- Compliance relevance

Only then does an inventory list become a reliable asset register.

2.3 Roles & Responsibilities in a CSAM Framework

A centralized asset register can only function reliably **when responsibilities are clearly defined**. Every security-relevant asset and object requires a clearly assigned owner—whether from a business, technical, or organizational perspective.

Without clear ownership, data maintenance becomes inconsistent and responses to changes or incidents are delayed. Effective Cybersecurity Asset Management deliberately distributes responsibilities across strategic, operational, and oversight layers. The illustration below shows a typical model where these layers converge.

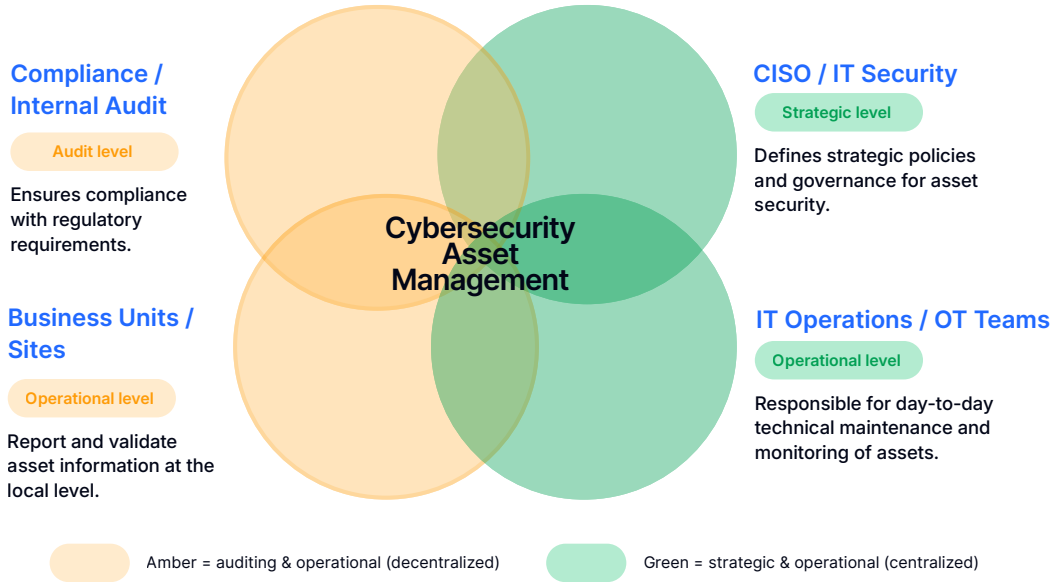
CSAM connects the strategic responsibilities of the CISO and information security function with the operational activities of IT/OT teams and business units, while incorporating compliance and internal audit as oversight functions within a shared governance framework.

In the illustration, orange represents decentralized operational and oversight responsibilities, while green represents centralized strategic and operational responsibilities.

What is Cybersecurity Asset Management (CSAM)?
Definitions & Scope

Role Model in Cybersecurity Asset Management

CSAM combines strategic, operational, and auditing responsibilities within a unified model.



2.4 Maturity Model for Cybersecurity Asset Management

Organizations vary significantly in their level of Cybersecurity Asset Management maturity. Before investing in additional software, it is therefore worthwhile to assess an organization's current state. **A simple maturity model can help establish a realistic baseline.**

Level 1 – Fragmented

- Asset data resides in spreadsheets or isolated tools
- No complete visibility across IT and OT systems
- Ownership is unclear or absent
- Data is frequently outdated

Typical question:
"Can we confidently say which systems actually exist?"

Level 2 – Consolidated

- Initial centralized inventories or CMDB structures exist
- Asset discovery is partially automated
- Basic security information is integrated
- Gaps and information silos remain

Typical question:
"Is our data current and complete enough to support security decisions?"

Level 3 – Managed

- Clear processes and responsibilities are defined
- Security KPIs are actively monitored
- Asset data supports patching, risk management, and incident response
- Regular quality controls are in place

Typical question:
"Can we identify affected assets quickly during an incident?"

Level 4 – Integrated

- Asset management is fully embedded within security and compliance processes
- High data quality and continuous updates are available
- Automated workflows and governance processes are in place
- Audit-ready evidence available at all times

Typical question:
"Are we actively using asset data to manage risk and compliance?"

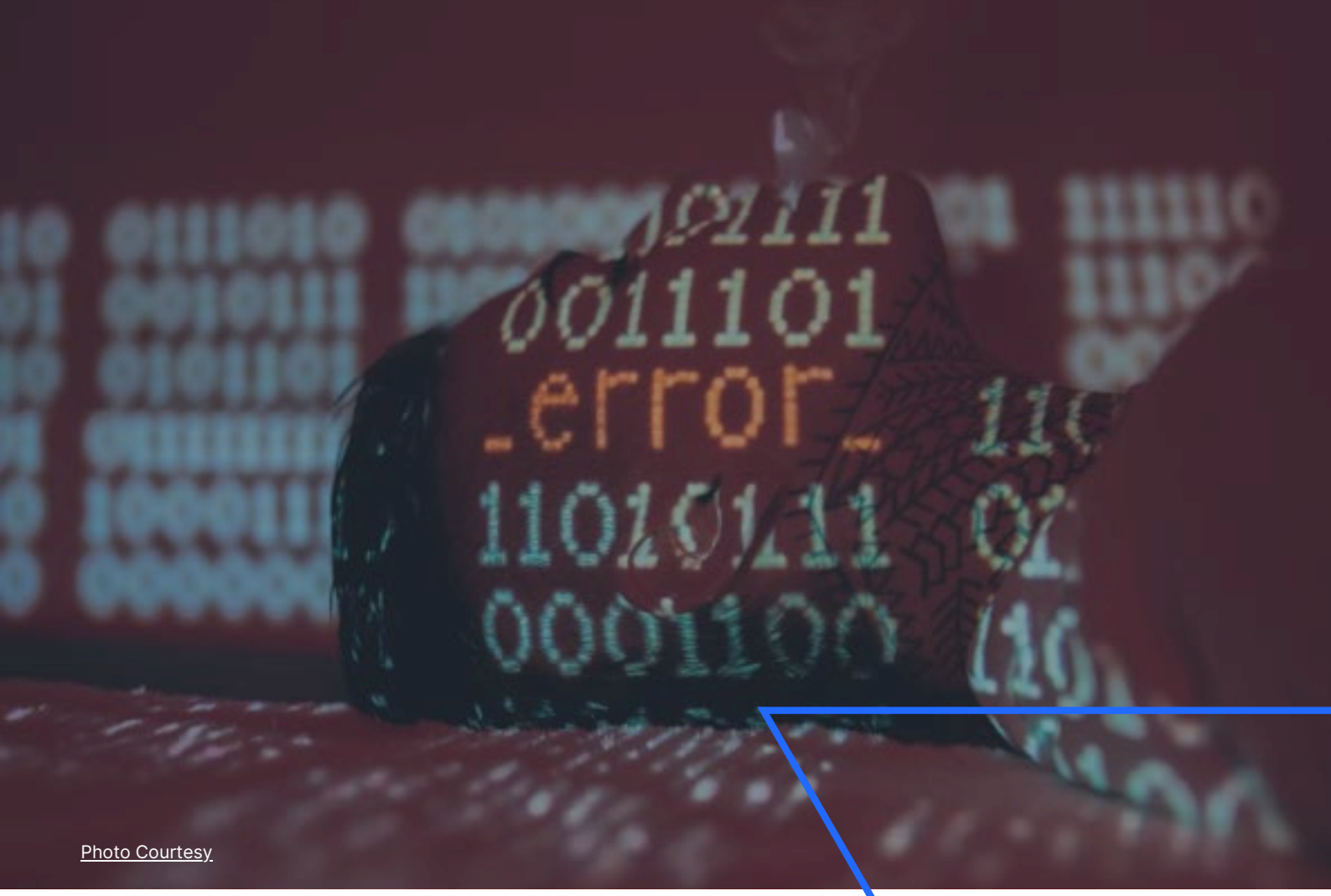


Photo Courtesy

Cybersecurity Asset Management

Problem & Context

Cybersecurity Asset Management: Problem & Context

In most organizations, the problem is not a lack of data—it is a lack of consolidation. CMDBs, discovery tools, cloud portals, and local inventories often coexist without creating a consistent, unified view. At the same time, IT and OT environments are expanding faster than inventories can be updated: new locations, short-lived cloud resources, external service providers, and unmanaged endpoints.

The result is unclear ownership, growing security blind spots, and an attack surface that few people fully understand. This chapter examines where traditional approaches fail and the specific risks that emerge as a result.

3.1 Growing Complexity of IT and OT Environments

Most organizations no longer operate within a clearly defined, centrally managed IT environment. Instead, their environments consist of a **mix of traditional office IT, cloud services, mobile endpoints, SaaS platforms, identities, network infrastructure, partner access, and—depending on the industry—OT components** such as machinery, control systems, sensors, or building automation. This heterogeneity is particularly pronounced in construction, manufacturing, facility management, and technical service organizations.

Operational dynamics add another layer of complexity. New construction sites are established, temporary networks are deployed, service providers receive access, new SaaS tools are adopted without centralized approval, cloud resources are provisioned quickly, and existing systems remain in service longer than planned. As a result, asset inventories are constantly shifting, often faster than centralized inventories or governance processes can be updated.

The outcome is unclear ownership and growing security blind spots. A system may technically exist but never appear in a centralized register. A device may be known but not assigned to a current owner. An application may be active, yet its criticality or patch status may not be properly documented. This is precisely where the core challenge of Cybersecurity Asset Management begins.

3.2. Why Traditional Inventories (Spreadsheets, Isolated CMDBs, Network Tools, and Cloud Portals) Are No Longer Sufficient

Most organizations already have numerous sources of information, ranging from CMDBs and discovery tools to cloud and endpoint platforms, IAM solutions, and security systems. The problem is usually not a lack of information but a lack of consolidation.

> Traditional inventories generally fail not because data is missing, but because they lack timeliness, consistency, and security context.

As described in Section 2.1, CSAM focuses on the risk-oriented and consistent representation of security-relevant assets. This is exactly where many traditional approaches struggle in practice, particularly when updates are performed manually or when new asset types emerge outside historical data models.

The limitations become especially apparent in CMDB-centric approaches. In static or rigid data models, cloud-native, short-lived, external, or business-unit-managed assets can easily remain invisible.

At the same time, direct visibility into patch status, vulnerabilities, exposure, identities, incident history, or data criticality is often lacking. Security platforms also typically provide only partial perspectives on assets and therefore require consolidation.

> A centralized asset register—such as one maintained within an asset management platform like Timly—creates a consistent and operationally useful view for security, compliance, and governance.

3.3 Consequences for Security & Compliance

Attackers deliberately target systems that are unmonitored, forgotten, or insufficiently secured. Particularly critical examples include:

- Outdated systems
- Unknown network devices
- Undocumented cloud services
- Unmanaged endpoints
- OT components without clear ownership

Typical consequences include:

Extended incident response times

During security incidents, organizations often lack immediate information about affected systems, ownership, and dependencies.

A high number of unknown assets

Organizations are often unable to reliably determine which systems are actually connected to their networks.

Incomplete patch coverage

Systems remain unpatched because they are unknown or not clearly assigned to a responsible team.

Audit and compliance gaps

Evidence related to ownership, security controls, or coverage often has to be compiled manually.

An expanded attack surface

Unknown or unmanaged assets directly increase the attack surface.

As a result, insufficient visibility into assets remains one of the most significant structural risk factors in modern IT and OT environments, directly affecting **threat detection, response speed, and compliance readiness**.

Photo Courtesy

Standards & Regulatory Requirements for the Asset Register

Standards & Regulatory Requirements for the Asset Register

For many organizations, regulatory requirements related to asset management are no longer an abstract future concern. **ISO 27001, NIS2, and other frameworks** all share the same fundamental expectation: organizations must be able to demonstrate which assets they own, who is responsible for them, and what security condition they are in.

A centralized asset register is therefore not an optional enhancement or a nice-to-have. Instead, it is a regulatory necessity. This chapter explains what the most important standards specifically require and where their expectations overlap.

4.1 ISO 27001: Inventory of Information and Assets

ISO/IEC 27001 makes it clear that information security cannot be implemented effectively without understanding which assets require protection. In particular, Annex A 5.9 requires the **systematic inventory of information and related assets**, as well as the assignment of clear ownership responsibilities.

Within the ISO framework, an asset register is therefore not an optional supporting tool but a fundamental prerequisite for risk assessment, security controls, and accountability within an ISMS.

What matters is not only the existence of an inventory, but also its quality. Annex A 5.9 assumes that inventories are **maintained consistently, remain current, and are traceable throughout the entire asset lifecycle**. In practice, this means the register must be properly maintained, include minimum required attributes, and be regularly reconciled with other records.

From an ISO perspective, a robust asset register should be able to answer the following questions:

- Which assets are within the scope of the ISMS?
- Who is responsible for each asset?
- How are criticality and protection requirements classified?
- How are new, modified, or retired assets reflected in the register?
- How are asset records systematically linked to risks, controls, and evidence?

Typical audit questions include:

- How do you ensure the completeness and accuracy of the register?
- How is ownership maintained throughout the asset lifecycle?
- Which asset classes are included within the ISMS scope, and why?
- How are asset records linked to risk management and control activities?

4.2 NIS2: Asset Management as the Foundation of Risk and Incident Management

Regulatory requirements such as the European NIS2 Directive significantly increase expectations regarding visibility and risk management. NIS2 does not prescribe a specific tool or inventory platform. However, the directive requires organizations to implement "appropriate technical and organizational measures" to manage cybersecurity risks. [3]

In practice, this requires a **reliable overview of systems, services, and ownership responsibilities**. Without a consolidated asset view, core requirements can only be implemented to a limited extent, particularly in the areas of:

- Risk assessments
- Incident response
- Vulnerability management
- Business continuity
- Reporting obligations

Of particular importance is the ability to quickly identify affected systems during an emergency. Organizations must be able to determine:

- Which assets are affected
- Their level of criticality
- Which locations are involved
- Which dependencies exist

CSAM therefore becomes a key driver of regulatory resilience.

4.3 Other Standards & Customer Requirements (Overview)

In addition to ISO 27001 and NIS2, **numerous other standards** and customer requirements indirectly depend on a robust asset register. These include:

- SOC 2
- TISAX
- Industry-specific security standards
- KRITIS requirements
- Customer audits
- Internal governance requirements

Although these requirements are phrased differently, nearly all frameworks rely on the same underlying assumption:

Organizations must know which systems, data, and access points they actually possess and secure. A centralized, up-to-date asset register therefore becomes the common foundation for security, compliance, and operational management.

- BSI and KRITIS requirements in Germany
- ANSSI frameworks in France
- INCIBE-oriented requirements in Spain

As a result, organizations increasingly need a scalable, standardized asset management model that can support both global governance and local regulatory requirements.

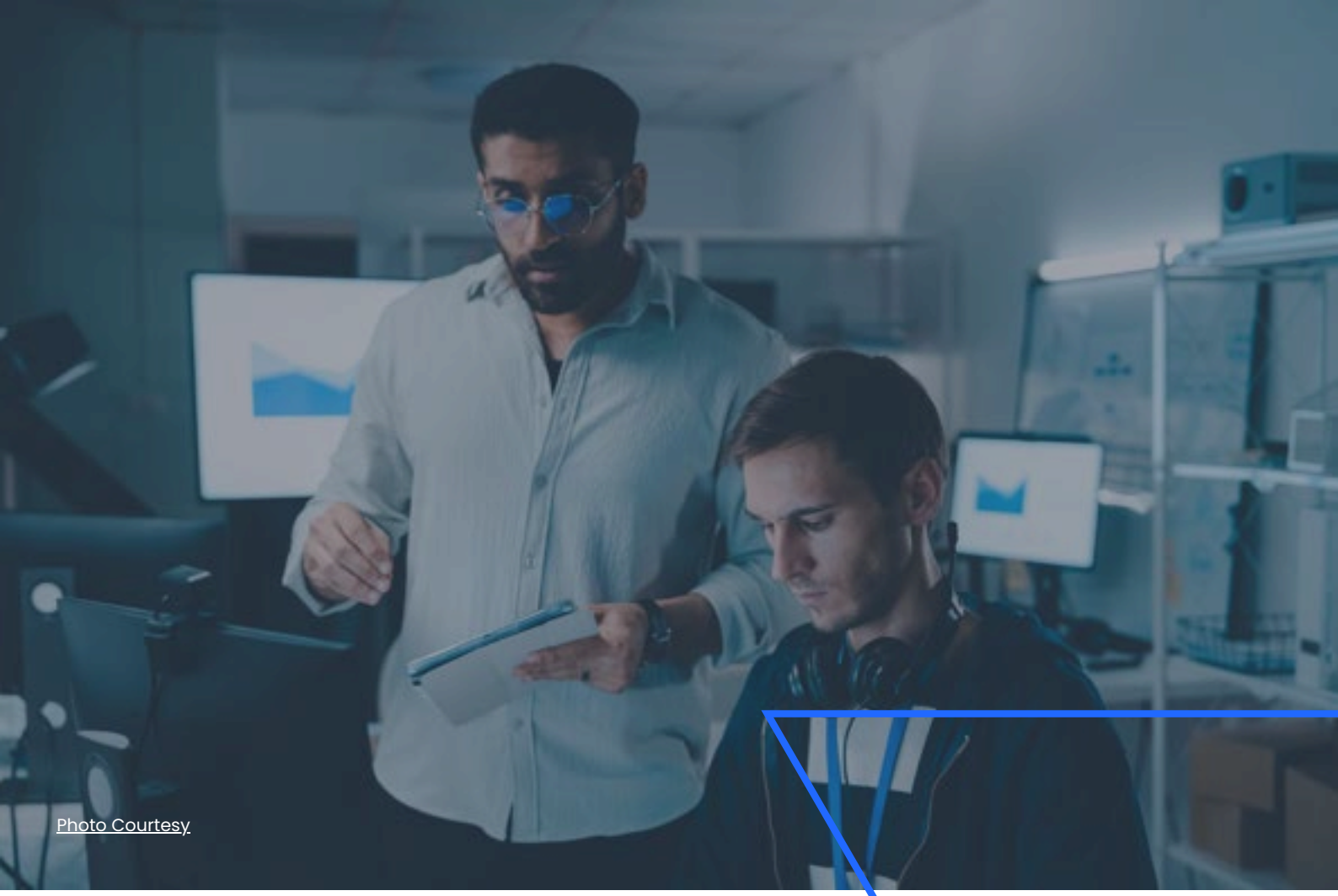


Photo Courtesy

Blueprint: Building a Security-Oriented Asset Register in 90 Days

Blueprint: Building a Security-Oriented Asset Register in 90 Days

In practice, a security-oriented asset register is rarely created through a single tool alone. What matters most is clearly **defining which systems are recorded, where the data comes from, who is responsible for it, and how it is maintained** on a day-to-day basis.

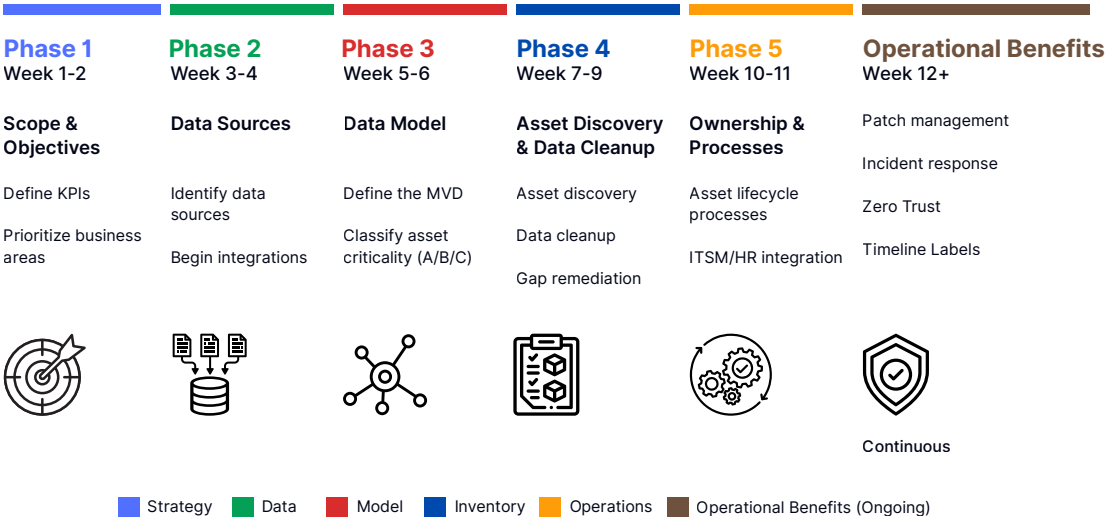
Unknown or unmanaged assets are among the most common security issues, as highlighted by analyses from Trend Micro and others. [4] For this reason, building an asset register should not be viewed simply as an IT inventory exercise. The primary goals are to:

- Improve visibility into attack surfaces
- Enable faster incident response
- Reduce audit-related effort

The following 90-day blueprint provides a pragmatic starting point. During the first 11 weeks (Phases 1–5), organizations define scope, connect data sources, establish a data model, conduct an inventory, and implement supporting processes. Beginning in week 12, the register becomes part of ongoing operational security activities.

The objective is not to document every asset perfectly from day one. Instead, organizations should take a **risk-based approach** that prioritizes the most security-critical areas first.

90-Day Roadmap: Building a Security-Focused Asset Inventory



5.1 Phase 1 – Define Scope & Objectives (Weeks 1–2)

Many projects fail before they truly begin because they attempt to create a complete inventory covering all systems, locations, and asset classes at once. In practice, this leads to lengthy discussions and significant effort before any usable results are achieved. **For a security-oriented asset register, a risk-based starting point is therefore recommended**.

During the first one to two weeks, the focus should be on **defining a clear scope and establishing measurable objectives**. Priority should be given to the systems and environments that are most important for threat detection, incident response, patch management, and compliance.

The illustration below highlights common starting areas that have proven effective in practice.

Blueprint: Building a Security-Oriented Asset Register in 90 Days

Typical Starting Points for Asset Inventory

Critical IT Systems

Servers
Databases

Exposed Endpoints

Mobile devices
Devices across multiple locations

Privileged Accounts

Administrators
System administrators

Core Network Infrastructure

Routers
Switches

Operational Technology (OT) Systems

Industrial control systems
Sensors

Cloud Services

Sensitive data
Broad access permissions

> *At the beginning, completeness is not what matters most. Connectivity is. A simple record containing an owner, location, and criticality rating is often enough to generate immediate security value.*
>
> **TIMLY CUSTOMER SUCCESS TEAM**

In distributed environments, such as construction, manufacturing, or facility management, it **may also make sense to include mobile or geographically dispersed assets early in the process** as these environments often experience visibility challenges and unclear ownership responsibilities.

At the same time, objectives should be defined as concretely as possible. Broad statements such as "improve visibility" are generally insufficient. **A small number of metrics that demonstrate progress and practical value are far more effective**. KPIs are particularly useful when they expose common weaknesses associated with incomplete inventories:

- unknown assets
- missing ownership assignments
- unclear patch status
- slow response times during security incidents

Initially, a **small KPI set** is sufficient to highlight visibility gaps and operational improvements. It should measure both the quality of the register and its practical contribution to security processes.

KPI	Why it matters?	Practical Target
Percentage of Unknown Assets	Shows security blind spots and potential attack surface.	< 5 %
Assets with an Assigned Owner	Required for accountability, remediation, escalation, and audit evidence.	> 90 %
Patch Visibility	Shows the percentage of assets with a reliable, up-to-date patch status.	> 95 %
Critical Assets with a Current Classification	Provides the foundation for prioritization in security and audit processes.	> 90 %
MTTR for Security Incidents	Measures how quickly affected assets can be identified and remediation can begin.	< 4 h (for critical incidents)

These values should not be viewed as rigid compliance requirements. They serve primarily as **guidance during the first 90 days**. Their true value lies in quickly identifying major gaps and determining whether the register is genuinely helping improve security operations.

Practical Tip

Without a clearly defined scope, organizations often end up with a register containing large amounts of data but little practical value. A risk-based approach helps close the most important visibility and security gaps first.

5.2 Phase 2 – Identify & Consolidate Data Sources (Weeks 3–4)

Once the scope has been defined, the next step is to connect the **most important data sources and bring them together into a unified view**. This phase should typically be completed during weeks 3 and 4.

Most organizations already possess significant amounts of asset information, but it is often spread across different systems such as Active Directory, cloud platforms, network tools, OT systems, and local inventory records.

> *The challenge is usually not a lack of data, but rather the ability to consolidate fragmented information into a consistent view.*

To get started, it is sufficient to **connect only the data sources that provide the greatest value** for security and visibility. These typically include:

- Active Directory or identity providers for users and permissions
- Network discovery tools for active devices
- Cloud platforms for virtual resources and services
- Existing asset or inventory repositories

These sources already provide a substantial portion of security-relevant information and help identify unknown or unmanaged assets. The combination of automated discovery methods, manual data collection, and QR/barcode scanning is discussed in greater detail in Phase 4.

Practical Example with Timly

Platforms such as Timly help combine technical discovery data with mobile inventory processes, QR/barcode scanning, and decentralized asset maintenance—particularly in distributed environments such as construction, manufacturing, and facility management.

The goal of this phase is not to collect every possible piece of information, but rather to **establish a centralized and usable view of the most important assets**. What matters is not that all data resides in a single system, but that information from multiple sources can be consolidated consistently.

Practical Tip

Many organizations attempt to integrate too many interfaces simultaneously. For an initial operational view, a small number of core sources, such as Active Directory, network discovery tools, cloud platforms, and existing inventory lists, is often sufficient. Additional data sources can be incorporated gradually over time.

5.3 Phase 3 – Define the Data Model & Minimum Data Requirements (Weeks 5–6)

Once key data sources have been consolidated, the next step is determining **which information is actually required for each asset**. This phase should be completed during weeks 5 and 6. Many inventories tend to become unnecessarily complex because too many fields are defined—fields that ultimately are not maintained in daily operations.

For a security-oriented asset register, a shared minimum data model is sufficient at the outset. Only information that is truly relevant for identification, ownership, prioritization, and security management should be captured.

This principle can be described as "**Minimum Viable Data**": as much information as necessary, but no more than required.

Minimum Data per Asset

Required Field	Why It Matters
Asset ID or unique identifier	Creates a clear reference and prevents duplicates
Asset type	Distinguishes, for example, IT, OT, software, cloud resources, or identities
Location or logical context	Shows where an asset is used or which domain it is assigned to
Responsible role	Clarifies accountability for assessment, actions, and escalation
Criticality	Helps prioritize based on risk and business impact
Security status	Makes patch level, audit status, or anomalies visible
Lifecycle status	Indicates whether an asset is active, changing, or decommissioned

These fields create a common foundation across different asset types. **Additional information can be added later** depending on the environment, such as manufacturer, serial number, firmware version, data classification, or associated vulnerabilities.

One of the most important minimum attributes is a simple **criticality rating** that helps prioritize assets within security and audit processes.

For most organizations, a practical three-level model is sufficient as a starting point:

Criticality Levels

Highly critical
Core systems, privileged access, sensitive data.

Important
Operational assets with noticeable impact if unavailable.

Supporting
Inventory-relevant assets with low priority in a security context.

A classification model of this kind establishes a common basis for risk assessments, patch prioritization, and incident response.

Criticality is not determined solely by asset type, but also by the asset's role within business and security processes. As a result, two technically similar devices may receive different classifications if one accesses sensitive data or supports a business-critical process.

Practical Tip

A small number of consistently maintained core fields is usually far more valuable than a complex data model that no one maintains properly.

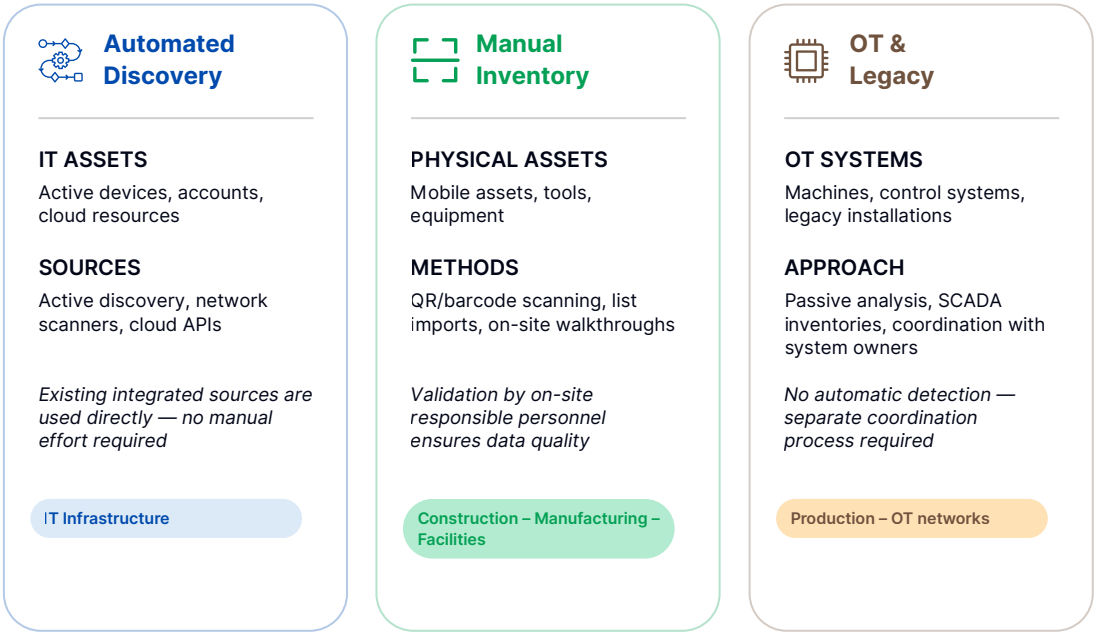
5.4 Phase 4 – Conduct the Initial Inventory & Data Cleanup (Weeks 7–9)

Phase 4 typically spans three weeks (Weeks 7 through 9) and is the most labor-intensive stage of the project. Once data sources have been connected and the minimum data model has been defined, the actual inventory process begins.

During this phase, technical and manual data collection methods are combined. Tools such as the Timly Inventory App can help establish a usable initial asset baseline as quickly as possible.

The following illustration shows the typical data collection methods that work together during this phase.

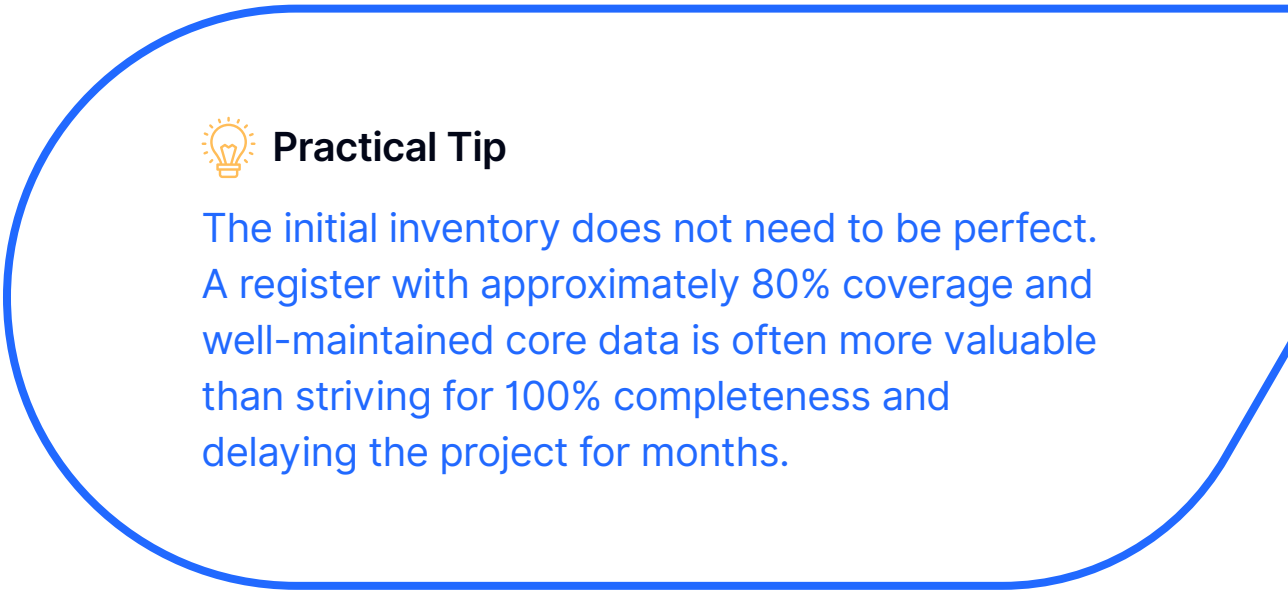
Data collection methods in Phase 4



After the initial data collection—whether through automated discovery, manual inventory processes, or separate OT procedures—the **data must be cleansed and standardized**. This includes:

- Resolving duplicates
- Completing missing mandatory fields such as owner, criticality, or location
- Closing obvious data gaps

The objective is not to create a perfect register, but rather a **functional baseline** that can already support security and compliance processes in a meaningful way. Remaining gaps can then be addressed incrementally as the register becomes part of daily operations.



Practical Tip

The initial inventory does not need to be perfect. A register with approximately 80% coverage and well-maintained core data is often more valuable than striving for 100% completeness and delaying the project for months.

5.5 Phase 5 – Embedding Responsibility & Processes (Weeks 10–11)

Weeks 10 and 11 focus on clarifying ownership and defining standard processes. A centralized asset register only delivers real value when it is **clearly defined who is responsible for an asset** and when any information must be updated. Without binding ownership responsibilities, even well-maintained registers quickly become incomplete or outdated. For that reason, this phase should not only define responsible parties, but also establish the most important processes surrounding the entire asset lifecycle.

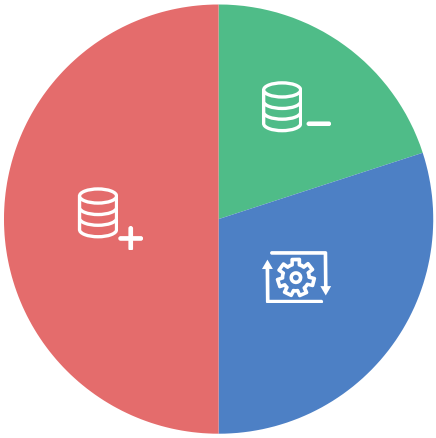
Three situations are particularly important in day-to-day operations:

1. **Onboarding**
2. **Changes**
3. **Decommissioning**

At each of these stages, the asset register must be maintained properly—from initial creation through modifications and eventual retirement. Asset maintenance should be integrated as closely as possible into existing ITSM, procurement, and HR processes so that updates occur naturally throughout the asset lifecycle.

The following illustration highlights these three key process moments.

Asset Lifecycle: The Three Key Process Stages



- **Onboarding**
  Create the asset, tag it, assign responsible owners, and record its criticality.
- **Change**
  Update the register with changes to location, usage, ownership, and status.
- **Decommissioning**
  Retire the asset, delete data, document evidence, and close the register entry.

Practical Example with Timly

To ensure asset data remains accurate over the long term, maintenance processes must be integrated as closely as possible into existing workflows. Mobile solutions such as Timly are particularly effective in supporting decentralized teams, maintenance activities, and cross-site asset ownership.

Common challenges include unclear responsibilities, insufficient prioritization, and limited visibility into operational benefits. For this reason, it should be clearly defined which event triggers which update and who is responsible for carrying it out. **Only clearly defined ownership and update processes can ensure long-term data quality**.

Practical Tip

Ownership only works reliably when asset maintenance becomes part of existing operational processes. Integration with ITSM, procurement, and HR workflows is particularly effective.

5.6 Operational Value: Security Use Cases (Beginning in Week 12)

After the implementation phase (Phases 1–5, weeks 1–11) has been completed, the asset register enters continuous operational use beginning in week 12.

A centralized asset register delivers its greatest value during day-to-day security operations. Processes such as patch management, incident response, and access control can only function efficiently when **accurate and reliable information about relevant assets** is available.

Without this foundation, security teams must manually collect information from multiple systems and spreadsheets whenever an incident occurs. With a centrally maintained register, affected systems can be **identified, prioritized, and managed much more quickly and consistently**.

The following three use cases clearly demonstrate the practical value of a centralized asset register.

Patch Management

When a critical vulnerability emerges, organizations without a centralized asset register often begin by searching for answers: Which systems are affected? Which versions are running where? Who is responsible? The required information is usually spread across multiple tools, lists, and teams.

With a centralized asset register, **affected systems can be filtered and prioritized immediately**—for example by software version, location, criticality, or owner. This makes it clear which systems require attention first and who is responsible for remediation. Patch status and remediation progress remain transparent and traceable.

Incident Response

During a security incident, such as a suspicious login or malware alert, it is often initially unclear which systems are affected and how serious the situation is. Without a centralized source of asset data, security teams frequently need to conduct manual investigations across multiple systems.

With an asset register, the **necessary context is immediately available**: the affected system, responsible owner, location, criticality, and potential dependencies. This allows initial containment measures to be initiated more quickly and escalation paths to be managed more effectively.

Access Control & Zero Trust

In many environments, access decisions are still based on simple assumptions such as network membership or VPN connectivity. The context surrounding the accessing system is often insufficiently understood.

An asset register provides the foundation required for context-based decisions by supplying information such as **device type, location, criticality, patch status, and ownership**. This enables more granular access controls, including restrictions for unknown or non-compliant systems.

Practical Tip

The operational value of an asset register is not measured by the amount of data it contains, but by the speed and quality of decisions it enables. What matters most is that the necessary context is immediately available during incidents, patching activities, and access-control decisions.

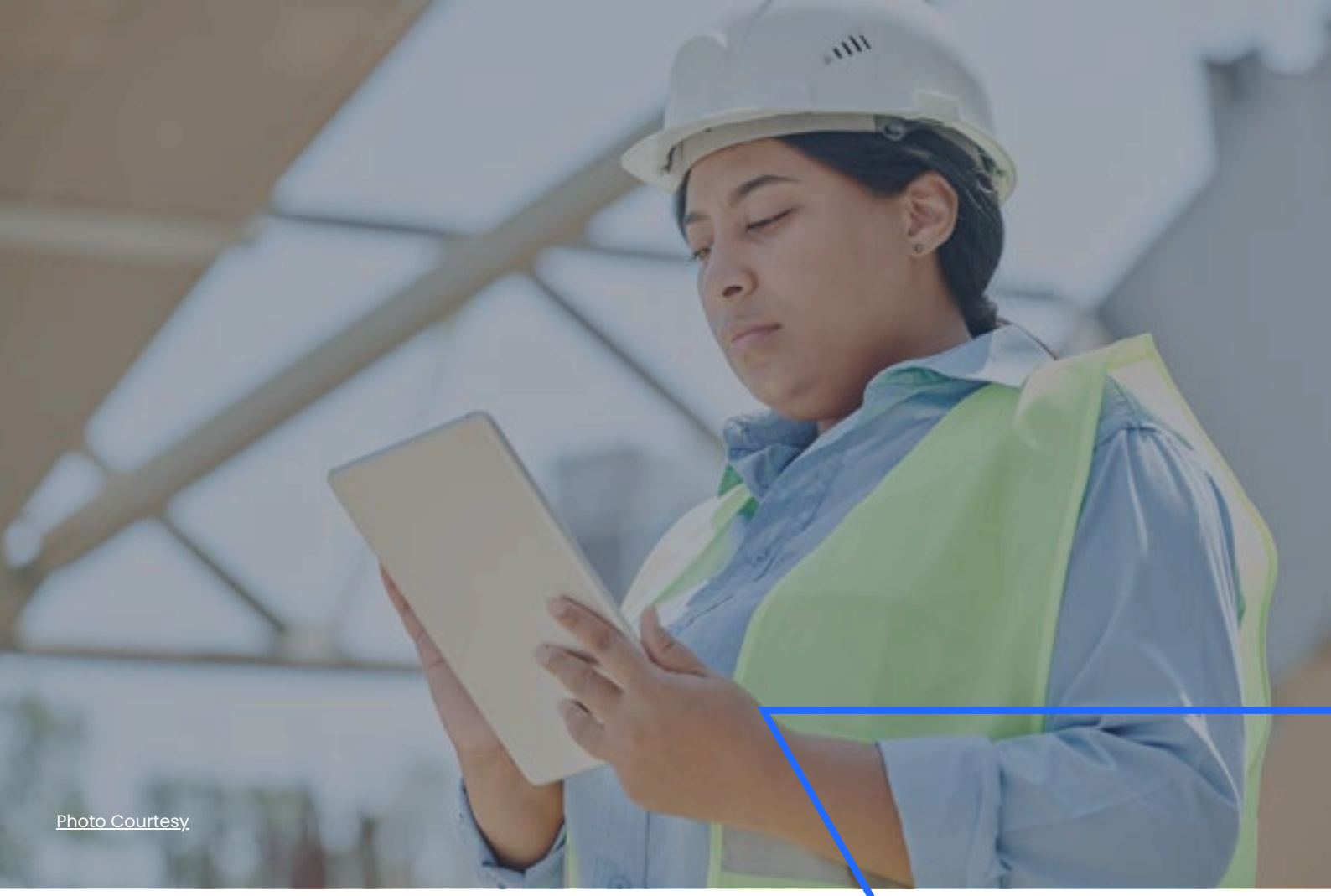


Photo Courtesy

Real-World Examples from Construction, Manufacturing, Facility Management & IT

Real-World Examples from Construction, Manufacturing, Facility Management & IT

The previous chapters explained how to build an asset register suitable for information security purposes step by step. The following examples demonstrate how this structure translates into day-to-day operational value across construction, manufacturing, IT, and facility management environments.

6.1 Mid-Sized Construction and Facilities Management Service Provider

Construction & Facilities Management Service Provider – 400 Employees, 30 Locations

Mobile assets, decentralized management via Excel & email

INITIAL SITUATION

Responsibilities were unclear, locations were not traceable, and audits were regularly incomplete. Several thousand mobile assets — tools, inspection devices, and IT equipment — were managed via decentralized lists, without reliable visibility into condition or whereabouts.

MEASURES IMPLEMENTED

- QR-based asset registration directly on-site across all locations
- Central assignment of responsible owners per asset
- Integration with identity management & ticketing systems
- A/B/C criticality model for maintenance prioritization

RESULTS

Unassigned assets
~18% → <3%

Incident response time
Days → <4h

Audit Readiness
First-time full compliance achieved
Inspection and accountability evidence directly available from the system

"The decisive moment is usually not the implementation itself, but the complete inventory. After that, it quickly becomes visible where clear ownership is missing."

– Timly Customer Success Team

6.2 Manufacturing Company With OT Focus

Manufacturing Company – OT Focus, Multiple Sites

Complex OT environments, parallel inventory lists, unknown firmware versions

INITIAL SITUATION

It was not documented which systems were truly critical — and therefore not determinable in the event of an outage. Parallel inventory lists were neither up to date nor consistent, and firmware versions were partially unknown.

MEASURES IMPLEMENTED

- Deliberately limited scope: prioritizing production-critical assets first
- Network discovery as the technical baseline inventory
- Manual enrichment of OT-specific data (firmware, manufacturer, area)
- Assignment of responsible owners and A/B/C criticality classification, integration with maintenance systems

RESULTS

Production-Critical Assets
>90% fully captured

Unknown Firmware Versions (high risk)
High → <5%

Vulnerability analysis
First-time prioritization possible
Affected systems identified and ranked by criticality within a short time

"In OT environments, the real problem is rarely the technology itself, but the lack of a shared view of which systems are truly critical."

– Timly Implementation Team

Real-World Examples from Construction, Manufacturing, Facility Management & IT

6.3 IT Service Provider / Managed Service Provider

IT Service Provider / Managed Service Provider – 50 customers

Heterogeneous IT environments, assets in ticketing systems, monitoring, distributed Excel files

INITIAL SITUATION

In an incident scenario, there was no consolidated overview across customers, systems, and responsibilities. Assets were distributed across different tools, and reporting required manual consolidation per customer.

MEASURES IMPLEMENTED

- Central register for internal and customer-related assets
- Automatic synchronization via RMM tools and cloud APIs
- Assignment of each asset to customers and internal responsible owners
- Standardized customer reports generated automatically from the register

RESULTS

Consistent asset coverage
>95% with assigned owner and customer reference

Incident identification
Hours → Minutes

Reporting
Fully automated
Regular customer reports run without manual effort

"The biggest difference is not created by more data, but by less time spent searching in an emergency."

– Timly Customer Success Team

Practical Takeaway

The examples reveal a recurring pattern: the greatest value does not come from achieving perfect completeness, but from establishing an early, usable structure with clear ownership responsibilities and consolidated core data. Once this foundation is in place, both operational security and day-to-day efficiency improve noticeably.

Photo Courtesy

Organizational Integration & Change Management

Organizational Integration & Change Management

One thing has become clear: An asset register does not create value simply through the implementation of a tool. Its effectiveness depends primarily on how well it is **embedded within existing ownership structures and operational processes**. The key success factor is integrating the register into established operational and governance processes.

This transforms the register from a simple information database into an operational point of reference for security, IT operations, and compliance.

7.1 Governance & Operating Model

Strategic responsibility for the asset register typically resides with IT leadership or the CISO function. This role defines the scope, minimum data model, criticality framework, and connections to risk and compliance requirements.

The primary responsibility at this level is not day-to-day maintenance but rather defining the rules according to which assets are classified and managed across the organization.

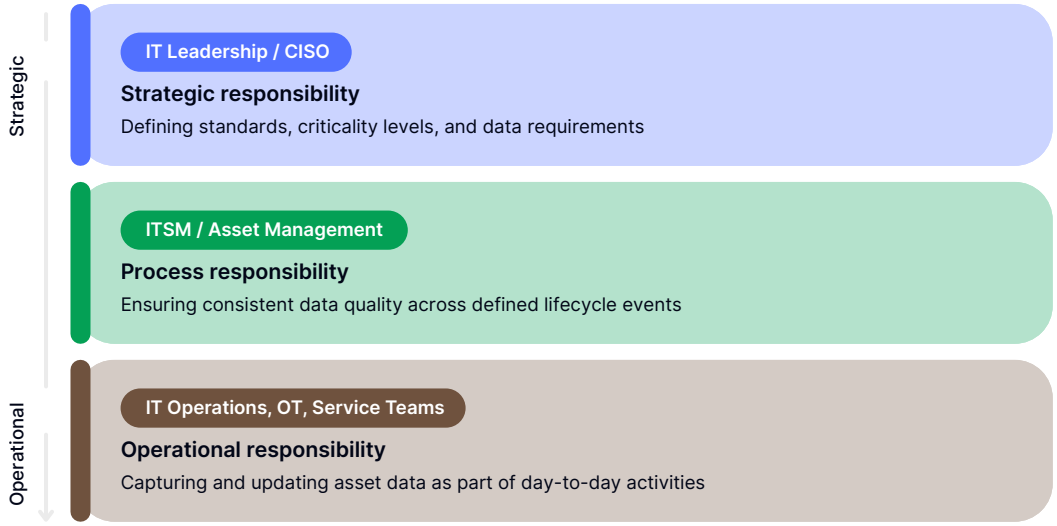
Operational responsibility lies wherever changes actually occur, including:

- IT operations
- OT teams
- Site organizations
- Technical service units

These groups are responsible for ensuring that asset-related events are immediately reflected in the system, such as asset deployment, relocation, maintenance activities, or decommissioning. In practice, most inconsistencies do not arise from a lack of ownership, but from unclear triggers and general uncertainty. Who records a change when a device is moved only temporarily? Who updates the register when a service is performed by an external provider?

A robust governance model therefore distinguishes not only between organizational levels, but also between different types of responsibility. The following illustration shows the three primary responsibility layers within an asset register.

Responsibility Levels in the Asset Register



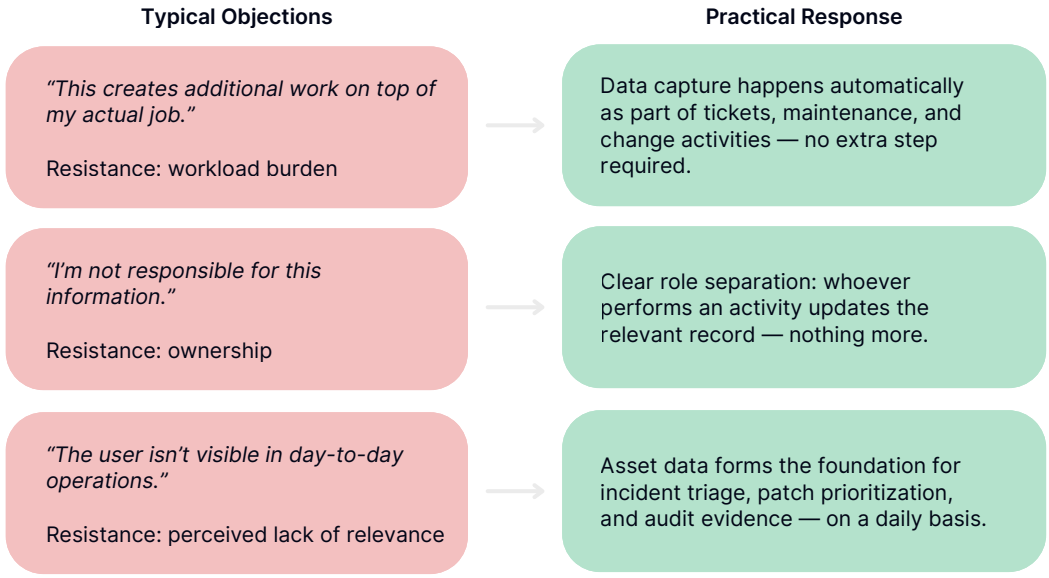
Organizational Integration & Change Management

7.2 Enablement & Everyday Adoption

The implementation of an asset register rarely fails because of technology. More often, it fails because of the **additional burden** it places on day-to-day operations. Common feedback from operational teams includes:

- "We already have enough work as it is."
- "That information isn't my responsibility."
- "I don't see any practical benefit for my team."

Adoption occurs primarily when asset data can be maintained directly within operational workflows. The illustration below shows **three common objections and practical ways to address them**.



The model only becomes effective when data collection and maintenance are integrated into existing processes.

In practice, relevant asset information should ideally be generated as part of normal operational activities—for example during ticket processing, maintenance work, change requests, or procurement activities.

The most effective approaches are those that minimize operational effort:

- **Mobile data capture and QR/barcode scanning** simplify inventory and maintenance activities in day-to-day operations.
- A **small number of mandatory core attributes** lowers the barrier to entry and improves data quality.
- **Embedding asset information into the operational context** helps support practical decisions, such as incident triage, patch prioritization, or audit preparation.

> *Adoption is not created through training. Instead, it is created through simplicity. When teams can register an asset in ten seconds using a QR code and immediately see the result reflected in a ticket or maintenance schedule, data maintenance becomes a habit rather than an additional task.*
>
> **TIMLY CUSTOMER SUCCESS TEAM**

7.3 Integration with Existing Management Systems

An asset register delivers its greatest value when it functions as the **central point of reference between existing operational, security, and compliance systems**.

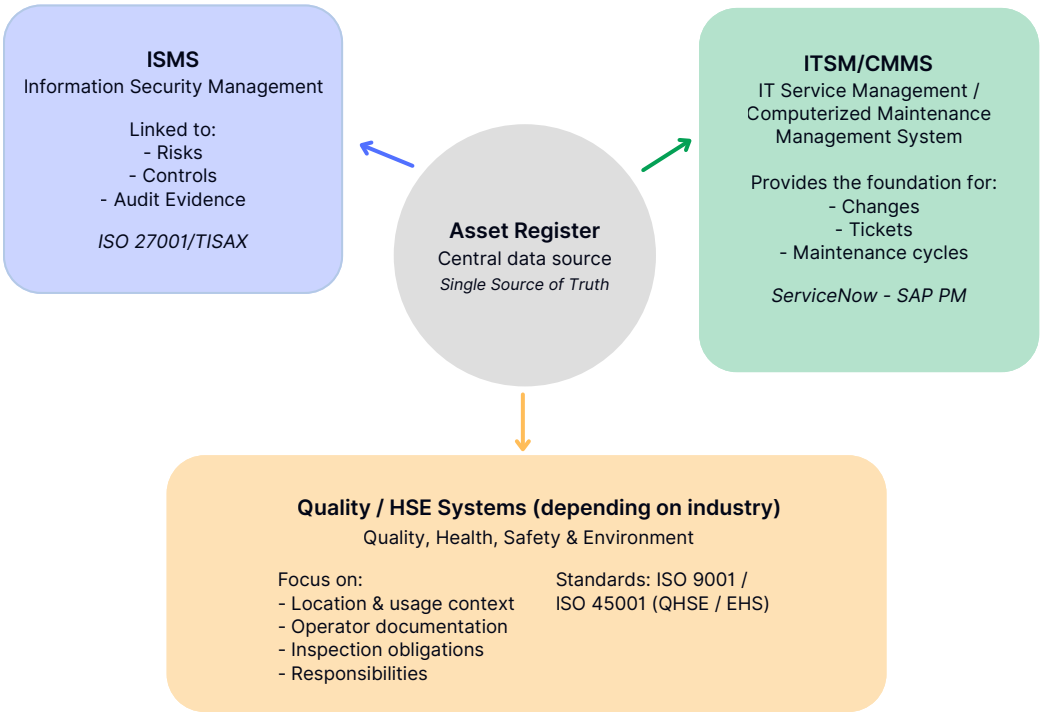
At the core are integrations with three key system categories:

ISMS Connects assets with risks, security controls, and audit evidence.

ITSM/CMMS
Uses the asset register as the foundation for change requests, tickets, and maintenance cycles.

Quality and HSE systems
Depending on the industry, these systems ensure traceability of location, usage, and ownership responsibilities.

The illustration below demonstrates how the asset register serves as the central data source connecting these systems.



It is essential to define a **clear system of record for each category of data**. Without this clarity, conflicting information quickly emerges between ITSM platforms, CMMS solutions, and the asset register itself.

Success depends on clearly defined roles and a well-defined interaction model among systems. The asset register serves as the central reference point, while operational systems provide updates and lifecycle events.

Typical organizational success factors during rollout include:

- Clear ownership responsibilities throughout the entire asset lifecycle, from onboarding through decommissioning.
- Integration into onboarding, change management, and decommissioning processes.
- Low barriers to adoption through a minimal set of required attributes.
- Early visibility into operational benefits, such as faster audits and fewer operational inquiries.

Photo Courtesy

Key Findings & Recommendations for Decision-Makers

Key Findings & Recommendations for Decision-Makers

The following key findings and recommendations summarize the most important insights from this report and highlight the actions organizations should prioritize in order to establish effective and sustainable Cybersecurity Asset Management.

8.1 The Five Most Important Takeaways

A robust asset register forms the operational foundation of modern cybersecurity and compliance processes. **The following key findings summarize the most important conclusions of this report:**

1. Without **consistent and well-maintained asset data**, effective cyber risk management is only possible to a limited extent. Unidentified or poorly managed systems remain among the most common causes of security gaps, delayed incident response, and incomplete patch coverage.
2. **Regulatory requirements such as NIS2 and ISO 27001** require traceable asset information, clear ownership responsibilities, and reliable evidence. Isolated inventory lists are no longer sufficient in dynamic IT and OT environments.
3. The greatest **value emerges during day-to-day operations**. A centralized asset register directly improves incident response, patch management, audit readiness, and security reporting.
4. Successful CSAM is therefore less about implementing a tool and more about **establishing governance, integrated processes, and continuous data maintenance**.
5. **Pragmatic implementation models** that focus on prioritized asset classes, a small number of core processes, and measurable improvements within the first few months tend to be the most effective.

8.2 Practical Recommendations for the Next 6–12 Months

Building an asset register suitable for information security should not be viewed as a standalone IT initiative. Instead, it should be approached as a gradual evolution toward a complete security-oriented operating model.

The following roadmap highlights the measures that have proven most effective in practice.

Quick Wins (0–3 Months)
(Corresponds to Phase 1–3 of the 90-Day Blueprint)

- Define critical asset classes and scope.
- Consolidate core data sources.
- Establish a minimum data model and ownership responsibilities.
- Implement initial security KPIs.

Operational Stabilization (3–6 Months)
(Corresponds to Phases 4–5 of the 90-Day Blueprint)

- Conduct the initial inventory and data-cleansing effort.
- Integrate the asset register with patch management and incident response processes.
- Embed ownership responsibilities throughout the asset lifecycle.
- Operationalize data quality management and update processes.

Strategic Development (6–12 Months)
(Expansion beyond the initial blueprint)

- Fully integrate the asset register into the ISMS.
- Automate audit and compliance reporting.
- Expand Zero Trust and risk-based decision-making capabilities.
- Continuously evolve the maturity model and governance framework.

Practical Tip

Organizations should avoid attempting to build a complete enterprise-wide inventory immediately. Iterative approaches that prioritize key asset classes and integrate core processes tend to be significantly more successful.

8.3 Outlook

Cybersecurity Asset Management is increasingly evolving from an inventory initiative into a central management layer for security, compliance, and operational resilience.

As regulatory requirements continue to increase through NIS2, ISO 27001, and industry-specific frameworks, organizations face growing pressure to demonstrate complete visibility into security-relevant assets. At the same time, hybrid IT/OT environments, cloud adoption, mobile work models, and external access requirements continue to expand.

As a result, a robust asset register will become an even more critical foundation for:

- Risk and compliance management
- Zero Trust architectures
- Automated vulnerability management
- Incident response and resilience
- Audit readiness and evidence management
- Integrated operational and maintenance processes

In the long term, modern CSAM approaches are evolving toward c**omprehensive operating models** that connect security, IT, OT, maintenance, compliance, and ESG-related processes within a unified framework.

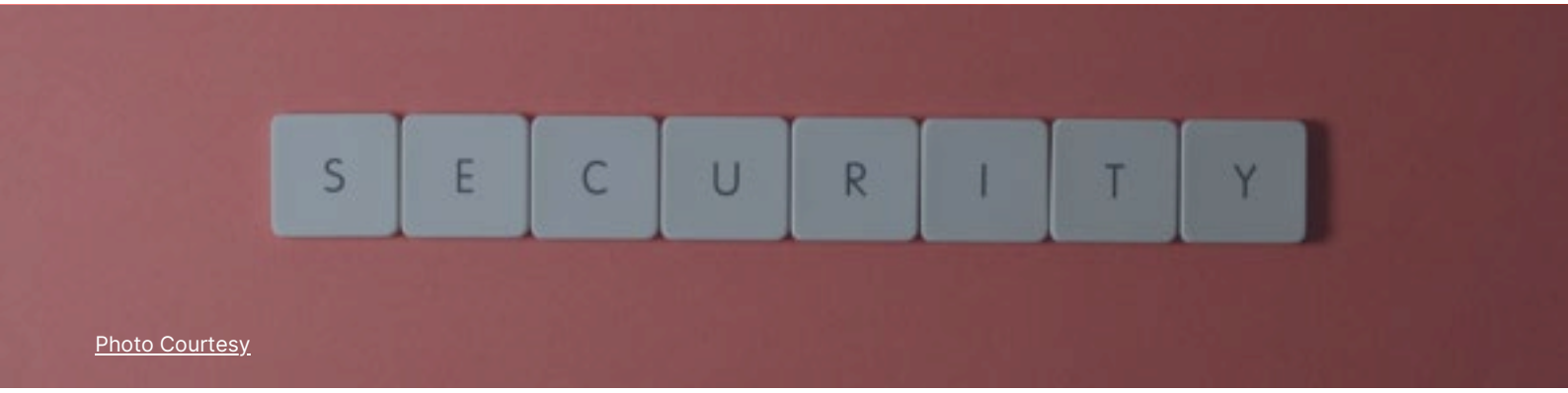


Photo Courtesy

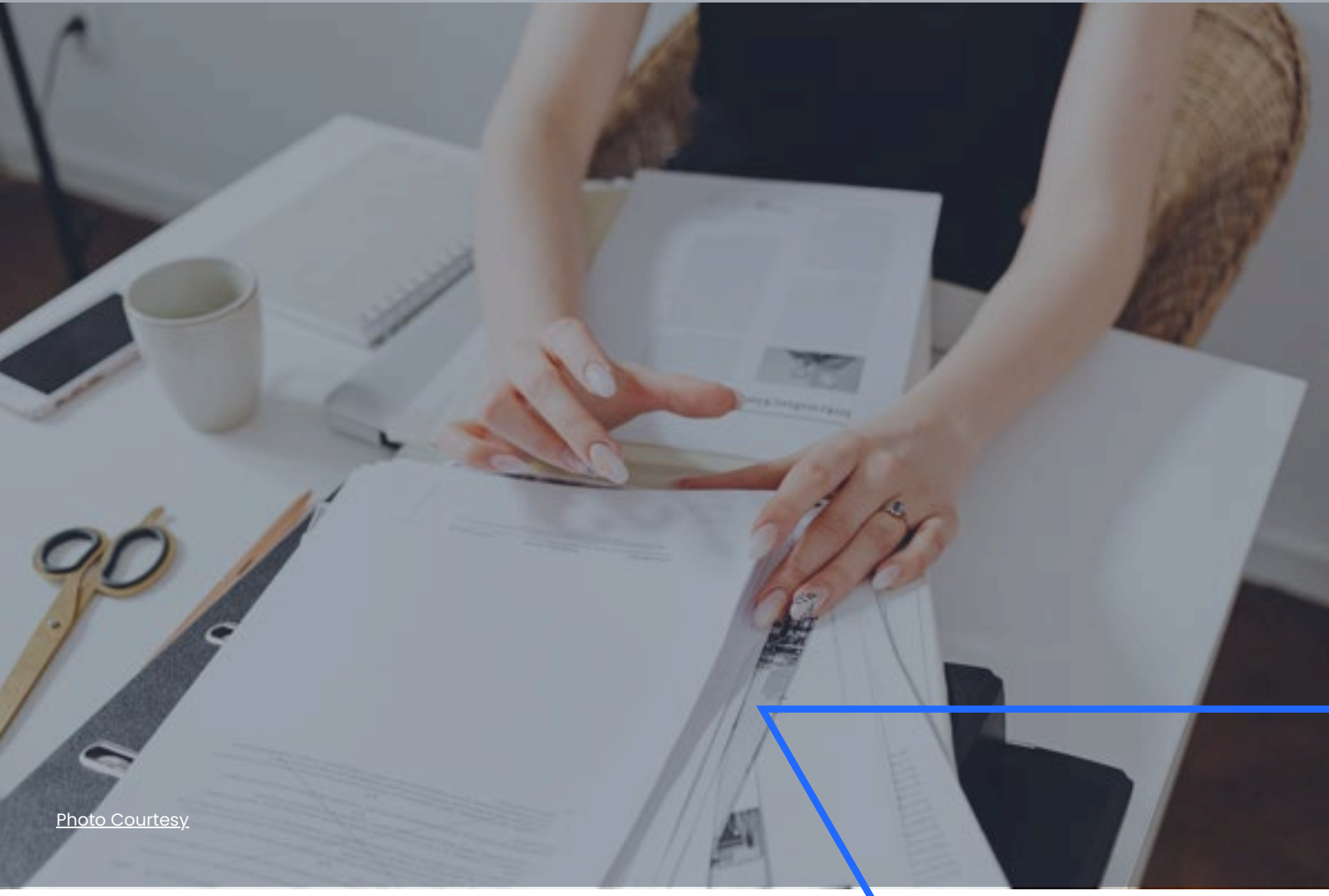
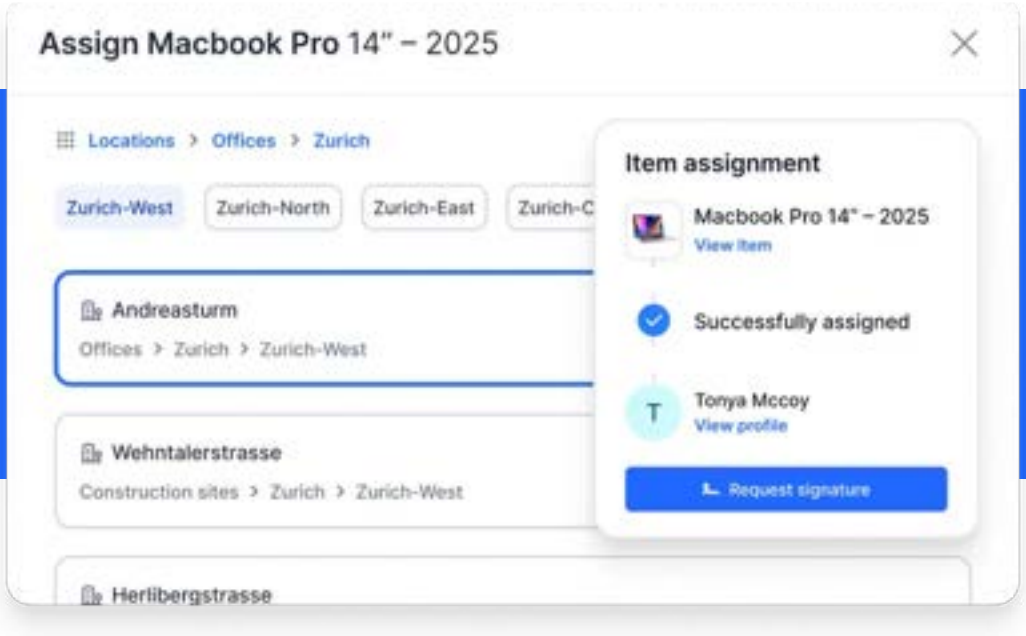


Photo Courtesy

About Timly & Methodology

Timly



About Timly & Methodology

Timly helps organizations centrally manage physical assets, operational equipment, and security-relevant resources in a transparent and mobile way. The asset management platform is particularly widely used in **industries with distributed and dynamic asset structures**, including construction, manufacturing, IT, facility management, technical services, and industrial operating environments.

A key focus is the connection between physical asset visibility, operational processes, and security-related requirements. This includes:

- Centralized management of physical assets and operational equipment.
- Mobile data capture using smartphones and tablets.
- QR code and barcode-based inventory management.
- Support for distributed locations and mobile teams.
- Integration of OT-related assets and technical equipment.
- Lifecycle and maintenance processes.
- Role-based ownership and accountability.

By combining simple data capture, mobile usability, and a centralized data foundation, Timly helps organizations **reduce visibility gaps and make asset information operationally useful** —both in IT/OT environments and for security, audit, and compliance requirements.

Learn how asset visibility can be implemented in distributed IT and OT environments through a free product demonstration.

BOOK A DEMO

9.1 Methodology

This report is based on a combination of:

- Publicly available studies and market analyses.
- Regulatory and standards-based requirements.
- Practical experience gained through customer projects.
- Internal insights from workshops, implementations, and user feedback.
- Operational observations from industries with distributed asset structures.

Among other sources, the report incorporates findings and requirements from:

- ISO 27001 / Annex A.
- The NIS2 Directive.
- Publications by Verizon, IBM, and other cybersecurity research organizations.
- Practical experience from IT, OT, and facility management projects.

The maturity models, KPI examples, and recommendations presented in this report are intentionally designed as a pragmatic target-state framework rather than a rigid compliance model. The objective is to provide organizations with a **practical starting point for building an asset register** suitable for information security purposes, with a focus on risk reduction, operational feasibility, and audit-ready transparency.

9.2 Sources

[1] https://www.verizon.com/business/resources/infographics/2025-dbir-infographic.pdf
[2] https://www.ibm.com/reports/data-breach
[3] https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[4] https://www.trendmicro.com/explore/aichangingcyberrisk