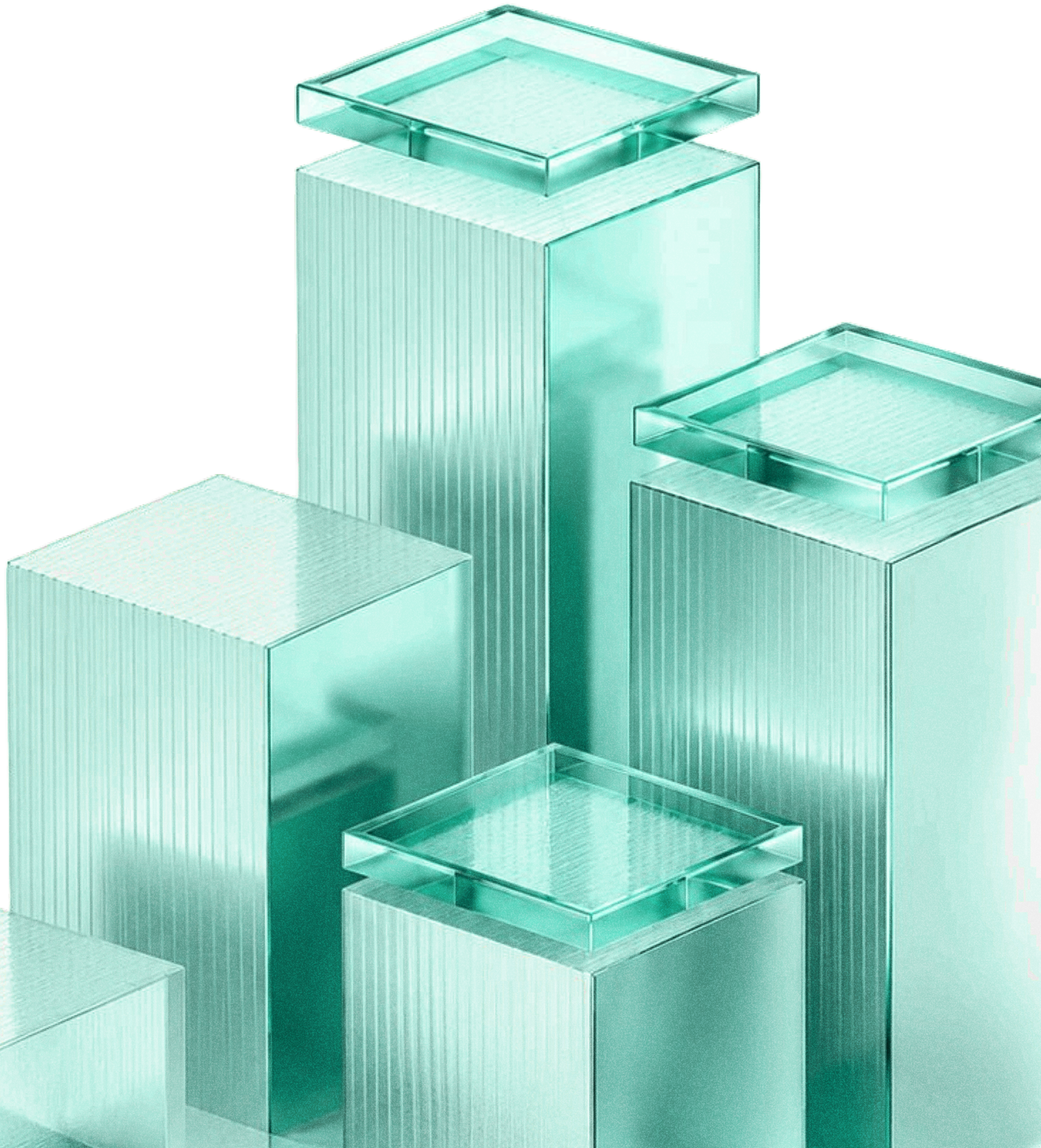
Teqtivity

DORA ICT Asset Readiness Assessment



Teqtivity

Table Of Contents

Are Your ICT Asset Records DORA-Ready?

Evaluate whether your ICT asset records are complete, current, and reliable enough to support governance, security alignment, and operational resilience.

A practical worksheet for security, IT, and operational leaders who need clearer asset data, stronger evidence, and greater confidence during day-to-day operations and disruption scenarios.

Why This Assessment Exists

Digital operational resilience depends on more than security tools and policies. Organizations also need accurate visibility into the ICT assets that support critical business operations, including who owns them, how they are governed, and how they change over time.

In many environments, asset data is spread across spreadsheets, procurement systems, endpoint tools, tickets, and disconnected workflows. Records may appear complete while still missing ownership, lifecycle history, operational context, or evidence.

This assessment helps security, IT, and operational leaders identify where ICT asset practices are strong, where records may be incomplete, and where better ITAM practices or tooling could improve governance, reporting, and resilience.

Important Note

This assessment is designed for internal evaluation and readiness discussions. It is not a certification, legal determination, or compliance opinion. It is a practical starting point for identifying strengths, gaps, and opportunities to improve.

How To Use This Assessment

For each statement, rate your process:

Score	Rating	Meaning
0	Not Started	No defined process or practice exists.
1	Planned	Requirements are understood but not consistently implemented.
2	Developing	Controls exist but coverage is incomplete.
3	Implemented	Practices are documented and generally followed.
4	Measured	Controls are reviewed, maintained, and supported by evidence.

Add your scores after each section and calculate your total at the end.

The goal is not a perfect score.

The goal is understanding whether your asset records support confident decisions during day-to-day operations and periods of disruption.

Assessment Sections

ICT Asset Visibility

Do we know what assets we have, where they are, and who uses them?

Relevant DORA themes: Article 6 (1), Article 8(1) (1), Article 8(4) (1), RTS Article 4(2)(b) (1)

We maintain a current inventory of ICT assets.

Asset records include ownership and location details.

Remote, distributed, and shared assets are included.

Asset records are updated after major changes, including procurement, deployment, reassignment, recovery, and retirement.

Asset records include relevant hardware, software, cloud services, and connected ICT services.

Asset inventories are reconciled against source systems such as MDM, procurement, HR, and directory services.

TOTAL: ICT Asset Visibility

What this uncovers: Inventory completeness, source system alignment, and confidence in asset data.

Asset Classification & Criticality

Do we know which ICT assets support critical business services?

Relevant DORA themes: Article 6 (1), Article 8(1) (1), Article 8(4) (1), RTS Article 4(2)(b) (2)

Critical ICT assets are identified and documented.

Assets are linked to business functions or services.

Asset criticality influences decisions about monitoring, recovery, replacement, and risk treatment.

We review critical asset lists periodically.

Recovery requirements, such as RTO/RPO where applicable, are defined for critical assets.

Asset records show key dependencies, supporting systems, and related business services.

TOTAL: Asset Classification & Criticality

What this uncovers: Business mapping, resilience planning, and dependency visibility.

Ownership & Accountability

Does every material ICT asset have a clear owner or accountable team?

Relevant DORA themes: Article 5 (1), Article 6 (2), Article 8(1) (2), RTS Article 4(2)(b)(iv) (1)

Assets have assigned owners or accountable teams.

Ownership changes are documented.

Responsibilities are defined for asset ownership, updates, recovery, and approvals.

Asset accountability remains clear when employees change roles, teams, locations, or employment status.

Shared, loaned, and stored assets have designated accountability.

Ownership records remain aligned with employee onboarding, movement, and offboarding.

TOTAL: Ownership & Accountability

What this uncovers: Orphaned assets, ownership drift, retrieval exposure, and unclear accountability.

Lifecycle Governance

Are assets tracked from purchase to deployment, recovery, and retirement?

Relevant DORA themes: Article 6 (1), Article 8(1) (1), Article 8(4) (1), RTS Article 4(2)(a) (1), RTS Article 4(2)(b) (3)

Assets follow a documented lifecycle process.

Deployments and reassignments are recorded.

Recovery and retrieval processes are documented and tracked through completion.

Retirement, disposal, and data sanitization activities are documented where applicable.

Procurement, receiving, and provisioning records connect to asset records.

End-of-support and end-of-life dates are tracked, reviewed, and used for refresh planning.

TOTAL: Lifecycle Governance

What this uncovers: Ghost assets, recovery gaps, refresh planning needs, and supplier support exposure.

Security Alignment

Are asset records connected to patching, monitoring, access, and risk controls?

Relevant DORA themes: Article 6 (1), Article 7 (1), Article 8(2) (1), Article 9 (1)

Asset records help security teams identify, prioritize, and investigate affected assets.

Devices can be matched against monitoring, MDM, endpoint security, or vulnerability management systems.

Access and ownership records align.

Asset information contributes to risk reviews.

Assets can be filtered or reported by compliance status, security posture, ownership, and criticality.

Security exceptions and remediation activities can be tied back to asset records.

TOTAL: Security Alignment

What this uncovers: Security visibility, remediation tracking, auditability, and risk context.

Resilience & Recovery

Do we know how critical assets will be restored if something fails?

Relevant DORA themes: Article 6 (2), Article 7 (1), Article 8(4) (2), Article 11 (1), Article 12 (1)

Critical asset records are used in recovery planning.

Teams can identify the assets, owners, and dependencies needed for restoration.

Asset dependencies are understood.

Recovery procedures are periodically reviewed.

Replacement assets, available stock, procurement paths, or alternate recovery options are documented for critical needs.

Teams can quickly determine operational impact if an asset becomes unavailable.

TOTAL: Resilience & Recovery

What this uncovers: Operational continuity, replacement readiness, and impact awareness.

Reporting & Evidence

Can we prove our asset controls through reports, records, and supporting documentation?

Relevant DORA themes: Article 5 (2), Article 6 (3), Article 8(1) (3), Article 8(4) (2), RTS Article 4(2)(a) (1), RTS Article 4(2)(b) (4)

Asset changes are logged and retained.

Reports can be produced without manual reconstruction.

Documentation supports internal reviews and audits.

Governance processes exist to review, correct, and maintain asset data quality.

Asset records maintain historical ownership and status history.

Exceptions, missing data, and corrective actions are assigned, tracked, and resolved.

TOTAL: Evidence & Governance

What this uncovers: Audit readiness, evidence maturity, and operational discipline.

Results & Interpretation

After completing the assessment, add your scores across all seven sections to get a general view of how mature your ICT asset practices are today.

Section	Section
ICT Asset Visibility	/24
Asset Classification & Criticality	/24
Ownership & Accountability	/24
Lifecycle Governance	/24
Security Alignment	/24
Resilience & Recovery	/24
Reporting & Evidence	/24
Total Score	**/168**

This score is not a compliance determination. It is a practical indicator of where your asset records, ownership practices, lifecycle controls, and evidence may need stronger structure.

Use the ranges below to guide discussion, prioritize improvements, and decide which areas need attention first.

0–42 → Initial

Asset visibility and evidence are limited. Teams may rely on manual checks, scattered records, and individual knowledge to understand what assets exist, where they are, and who owns them.

43–84 → Developing

Basic asset controls exist, but they are not yet consistent across teams, systems, or lifecycle stages. Some

records may be useful, but gaps in ownership, updates, retrieval, or reporting can still create risk.

85–126 → Established

Asset governance is functioning and supports many day-to-day decisions. The next opportunity is to improve consistency, measurement, integrations, and evidence across the full asset lifecycle.

127–168 → Advanced

Asset controls are documented, maintained, and supported by reliable evidence. Your organization is better positioned to support ICT governance, security alignment, resilience planning, and internal readiness discussions.

Your Score Is A Starting Point

Operational resilience is built over time. Your score is meant to help you see where your ICT asset practices are strongest today and where they may need more attention.

A lower score does not automatically mean your organization is unprepared, and a higher score does not mean the work is finished. What matters most is whether your teams can trust asset data when decisions need to be made, especially under pressure.

Use your results to identify:

- Areas where asset visibility may be incomplete
- Processes that rely too heavily on manual effort
- Assets that lack clear ownership or lifecycle history
- Records that are difficult to prove during reviews or audits
- Opportunities to strengthen governance, resilience, and reporting

Choose one or two areas to improve first. Focus on the areas that create the most risk, require the most manual effort, or make reporting hardest to support.

Small, targeted improvements in asset accuracy, ownership, lifecycle tracking, and evidence can create meaningful gains in resilience over time.

Recommended Next Step

Review the two lowest-scoring sections first. These areas are likely where your ICT asset records create the most manual work, uncertainty, or reporting difficulty.

For each section, identify:

- What data is missing
- Which team owns the process
- Which systems should be connected
- What evidence needs to be easier to produce
- What can be improved in the next 30–60 days

Strengthen ICT Asset Governance

The strongest ICT asset programs are built on practices that keep records accurate, ownership clear, lifecycle activity visible, and reports ready when teams need them.

Teqtivity helps organizations connect asset data across systems, track lifecycle changes, and maintain the records needed to support governance, security alignment, and operational resilience.

See Teqtivity In Action →

Disclaimer

This assessment is provided for informational purposes only and is not legal, regulatory, audit, or compliance advice.