

Workforce Cyber Readiness in the NIS2 Supply Chain

A practical framework for current, verifiable workforce status
across flexible labour and supplier relationships

ENTERPRISE GOVERNANCE

controls · risk · suppliers

WORKFORCE READINESS

people · connections · status

TECHNICAL SECURITY

systems · telemetry · incidents

NIS2

CBW

WORKFORCE

SUPPLY CHAIN

CONTENTS

Workforce cyber readiness, from boundary problem to operating model

01 Executive summary	08 Language and high-turnover lifecycle
02 The supply chain has a human edge	09 Supplier demonstrability
03 What the Cyberbeveiligingswet changes	10 How the layers fit together
04 The workforce boundary changes faster than the evidence	11 Operator checklist
05 Seven questions a workforce evidence system should answer	12 Staffing agency and supplier checklist
06 Current status and portable credentials	13 The EdXactly model
07 Verification without surveillance	14 Conclusion and sources

The workforce moves across organisational boundaries faster than most evidence systems do.

Published 14 September 2026 · Last reviewed 14 September 2026 · Netherlands / EU NIS2

Executive summary

The Cyberbeveiligingswet has been in force in the Netherlands since **15 August 2026**.^[1] It brings the European NIS2 framework into Dutch law and strengthens expectations around cybersecurity risk management, governance, supply-chain security, cyber hygiene and the effectiveness of controls.^{[2][3]}

For many organisations, the technical and governance layers are already familiar.

Security operations teams manage systems, telemetry and incidents. GRC and third-party risk platforms manage frameworks, controls, policies, risks and suppliers.

A different problem appears when the organisation depends on people who sit outside its permanent workforce.

Agency workers, contractors, supplier personnel and other flexible workers can move between clients, sites and assignments without belonging permanently to any one client's HR, identity or learning environment. Their organisational relationship can change faster than a monthly spreadsheet, certificate bundle or manually maintained LMS record.

That creates a specific evidence question:

Which relevant people currently hold the workforce cyber-readiness status required for the work they are doing?

This is not the same as asking whether a supplier has a policy, whether a security control exists, or whether a person completed an activity in the past.

The workforce layer needs to connect seven things:

1. **Population** - who is relevant?
2. **Connection** - which organisation-worker relationship is active?
3. **Requirement** - what readiness status applies?
4. **Status** - has the worker earned it?
5. **Currency** - is it still valid now?
6. **Verification** - can an authorised party check it?
7. **Lifecycle** - what happens when the worker leaves, returns, expires or is revoked?

This paper sets out a practical framework for that layer.

It also makes an important boundary clear: workforce-readiness evidence can support NIS2/Cbw risk management and supplier demonstrability, but it does **not** by itself determine legal scope, certify compliance, replace technical cybersecurity measures or transfer responsibility between organisations.

Scope of this paper

This paper focuses on **workforce cyber-readiness evidence** in environments where people cross organisational boundaries.

It is particularly relevant to:

- staffing agencies;
- workforce suppliers;
- contractors;
- operators using multiple suppliers;
- sites with high worker turnover;
- organisations that rely on external personnel with access to systems, information or operational environments.

It is **not** a general guide to every NIS2/Cbw obligation.

It does not claim that:

- every supplier is automatically subject to the Cyberbeveiligingswet;
- every external worker needs the same programme;
- every staffing relationship creates the same cyber risk;
- one worker credential establishes legal compliance;
- a workforce register replaces a GRC, ISMS, SOC, IAM or third-party risk platform.

The legal and risk analysis remains organisation-specific.

The purpose here is narrower:

to define the evidence problem that appears when workforce status has to remain current across suppliers, clients and changing assignments.

1. The supply chain has a human edge

Cyber supply-chain risk is usually discussed in terms of technology.

The familiar objects are:

- software;
- cloud providers;
- managed services;
- network dependencies;
- ICT suppliers;
- vulnerabilities;
- third-party systems.

Those are essential parts of the risk picture.

But many services are delivered through people.

A supplier may provide personnel who:

- enter a client site;
- use client systems;
- handle client information;
- use scanners, terminals or shared workstations;
- receive access credentials;
- operate around production or logistics technology;
- change frequently.

The supplier relationship may be stable while the individual workforce inside that relationship changes every day.

That creates a distinction that traditional supplier governance does not always capture:

the organisation boundary and the workforce boundary are not the same.

A client may know that Supplier A is approved.

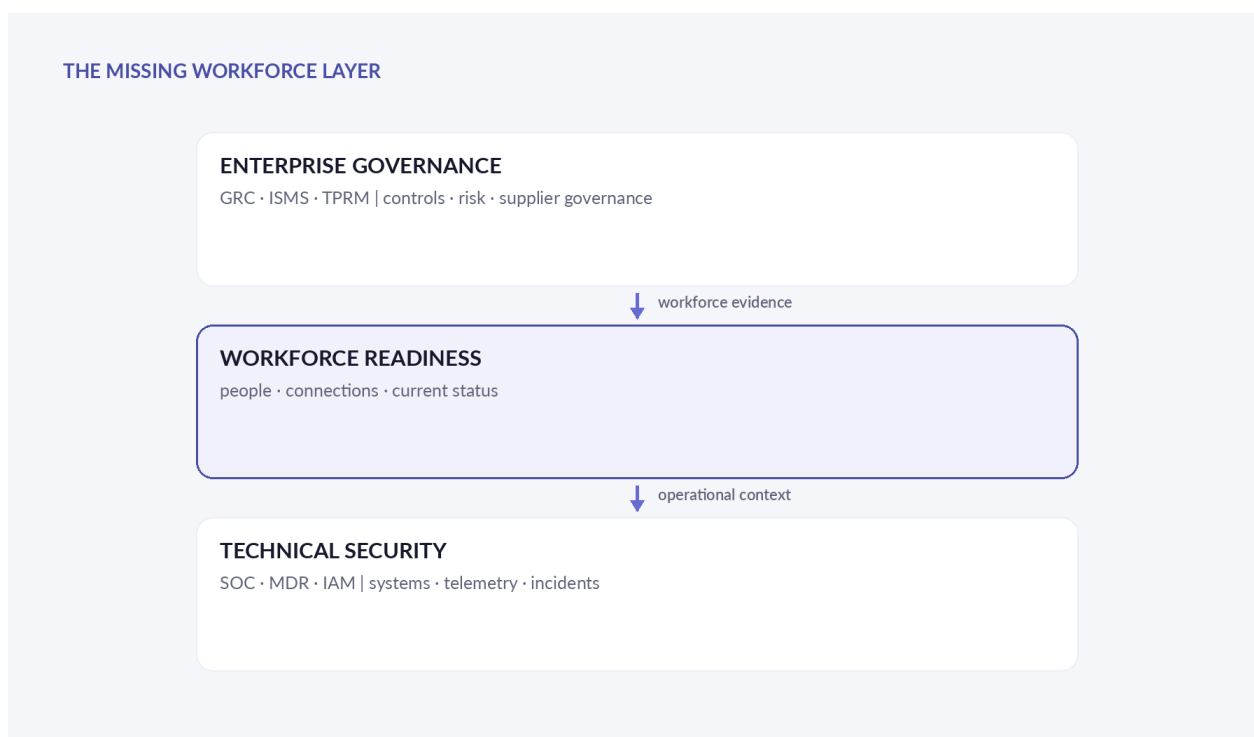
It may still need to know:

Which people from Supplier A are relevant today, and what is their current status?

That is a worker-level evidence problem inside an organisation-level supplier relationship.

<!-- FIGURE 1: editorial full-width diagram -->

Figure 1 - The missing workforce layer



The three layers solve different problems.

The workforce layer should integrate with the others where useful. It should not pretend to replace them.

2. What the Cyberbeveiligingswet changes

The Cyberbeveiligingswet entered into force on **15 August 2026**.^[1]

The NCSC describes ten duty-of-care measures and makes clear that organisations remain responsible for determining which measures are appropriate, with risk management as the basis.^[2]

Three areas are particularly relevant to this paper.

2.1 Supply-chain security

The NCSC identifies supply-chain security as one of the duty-of-care measures and advises organisations to include chain risks in risk management, map direct suppliers and strengthen supplier resilience through dialogue and appropriate measures.^[2]

The NCSC also states that a Cbw organisation can require cybersecurity measures from direct suppliers and service providers where the relationship is relevant to its network and information-system risks.^[4]

That point requires precision.

It does **not** mean every supplier automatically inherits the client's Cbw obligations.

NCSC guidance explicitly treats supplier impact as risk-dependent. A supplier whose products, services or access can affect a Cbw organisation's network and information systems is more likely to become part of that chain-risk analysis.^[4]

For workforce suppliers, the relevant question is therefore not:

"Are staffing agencies automatically subject to the client's obligations?"

It is:

"Does the supplied workforce create a relevant cybersecurity relationship, and if so, what evidence will the client reasonably require?"

That answer depends on the actual work, access, systems, information and risk.

2.2 Cyber hygiene and safe behaviour

The NCSC's Cbw guidance identifies cyber hygiene and cybersecurity training as a separate duty-of-care measure.^[2]

Its broader guidance on safe digital behaviour also emphasises that knowledge alone is not enough and that organisations should understand the actual behavioural problem they are trying to solve, measure interventions and combine human and technical measures.^[5]

The practical implication for workforce evidence is straightforward:

a record that an activity occurred is useful, but it is not the entire risk-management story.

2.3 Personnel and access security

The NCSC also identifies personnel, access policy and asset management as a Cbw duty-of-care area.[2]

That is relevant because external and flexible workers often sit exactly where these topics meet:

- personnel relationship;
- access;
- system use;
- changing assignments;
- onboarding and offboarding.

A workforce-readiness layer should therefore complement, rather than blur, the distinction between:

- who the person is;
- what access the person has;
- what readiness status the person currently holds.

3. The workforce boundary changes faster than the evidence

Permanent employees usually fit inside a relatively coherent organisational identity model.

They tend to have:

- an HR record;
- corporate identity;
- email;
- LMS profile;
- access-management lifecycle;
- stable organisational ownership.

Flexible workforces behave differently.

A worker may:

- spend two weeks at one client;
- move to another site;
- disappear for several months;
- return through the same staffing agency;
- work under a different assignment;
- use a different client system;
- never receive a permanent client identity.

That creates two common evidence patterns.

Pattern A - duplicate the worker into every client environment

The client creates:

- another directory identity;
- another LMS profile;
- another credential;
- another offboarding obligation.

This can be appropriate where the worker genuinely needs system access.

But it creates unnecessary identity sprawl when the account exists mainly to carry evidence.

Pattern B - keep the evidence outside the client environment

The supplier sends:

- spreadsheets;
- certificates;
- screenshots;
- LMS exports;
- email attachments.

This reduces account creation, but creates evidence sprawl.

The data is often correct only at the moment it was generated.

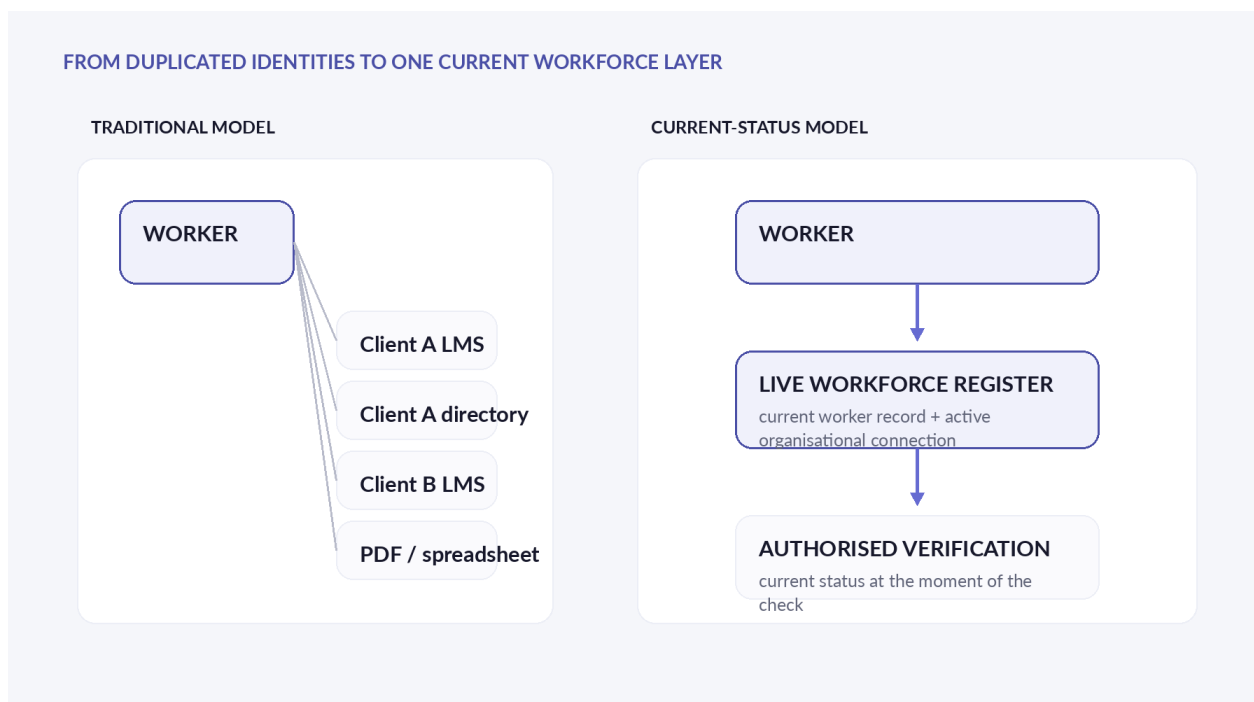
Neither pattern fully solves the current-status problem.

A third model is possible:

maintain the workforce status in a live register, connect it to the relevant organisational relationship, and let authorised parties verify the current state when needed.

<!-- FIGURE 2 -->

Figure 2 - From duplicated identities to one current workforce layer



The point is not that client identities disappear.

The point is that **readiness evidence should not be the reason another unnecessary identity is created.**

4. Seven questions a workforce evidence system should answer

A workforce cyber-readiness model does not need to begin with technology.
It can begin with seven questions.

1. Population

Who is actually relevant?

The population may include:

- permanent employees;
- agency workers;
- contractors;
- supplier personnel;
- temporary site workers;
- seasonal workers.

Not every person will have the same cyber relevance.

The organisation's risk analysis determines which workforce populations matter.

But unless the population is known, coverage cannot be demonstrated.

A percentage such as "90% ready" is meaningless if the denominator is unclear.

2. Connection

Which organisation-worker relationship is active?

The same person may be associated with:

- one staffing agency;
- several client organisations over time;
- a physical site;
- a supplier contract;
- a returning assignment.

The relationship matters because a readiness requirement exists in context.

The person alone is not the whole record.

The useful unit is:

person + active organisational connection.

3. Requirement

What does this connection require?

The requirement should reflect:

- role;
- system exposure;

- information access;
- organisational policy;
- identified risk.

The existence of a register does not remove the need for risk-based judgement.

A generic requirement may be appropriate in one environment and inadequate in another.

4. Status

Has the person earned the required status?

The method can include:

- training;
- assessment;
- acknowledgement;
- practical checks;
- other defined evidence.

The operational output should be understandable.

Where a client only needs to know whether the requirement is met, the external result can be a **status** rather than a detailed worker score.

5. Currency

Is the status still valid now?

Status needs a time dimension.

Relevant events can include:

- expiry;
- changed requirements;
- revocation;
- connection closure;
- revalidation.

A historical record can remain true while no longer being operationally current.

6. Verification

Can an authorised party check the current answer?

If every question triggers a new manual evidence request, the organisation still has an evidence-collection process.

A live evidence model should make the relevant current state directly verifiable where appropriate.

7. Lifecycle

What happens when the person leaves, returns or changes context?

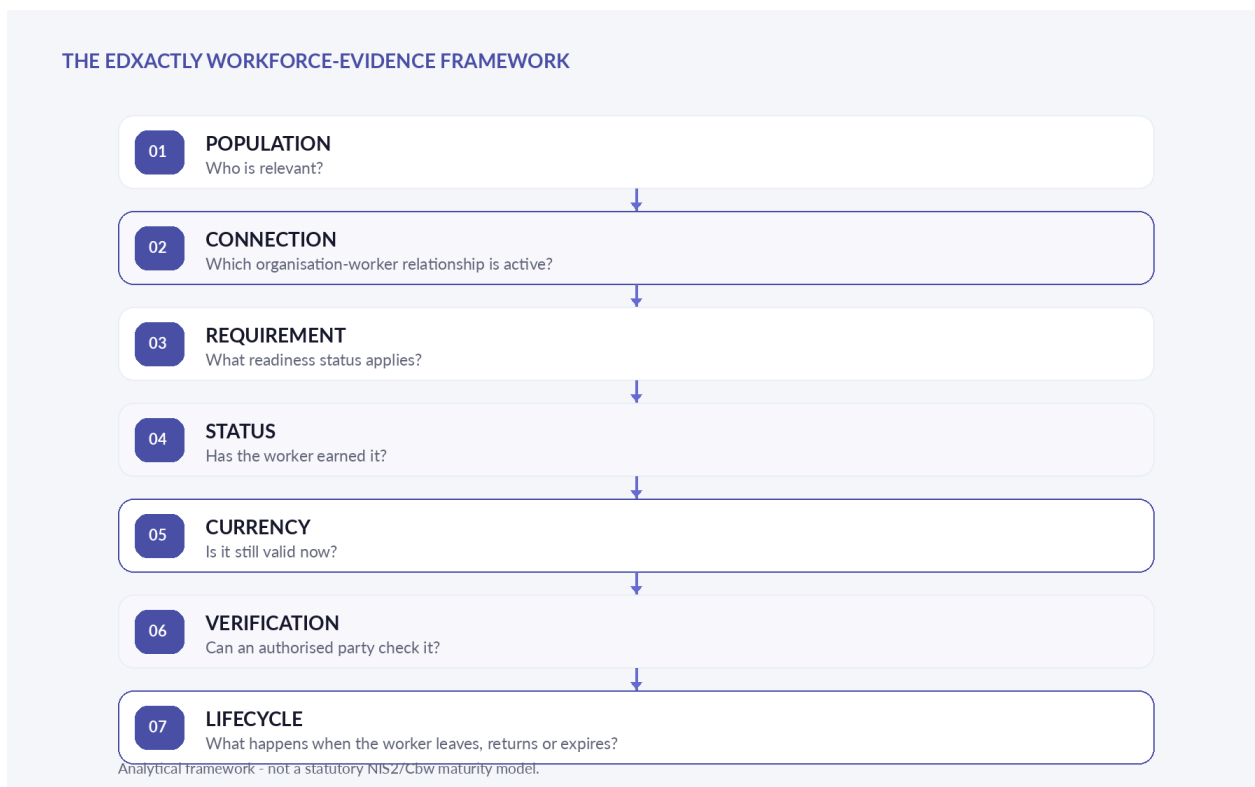
Flexible labour is defined by movement.

A readiness system should expect that.

It should not treat return as an edge case.

<!-- FIGURE 3 -->

Figure 3 - The EdXactly workforce-evidence framework



This framework is an EdXactly analytical model, not a statutory NIS2/Cbw maturity model.

5. Current status and historical evidence answer different questions

A historical record answers:

What happened?

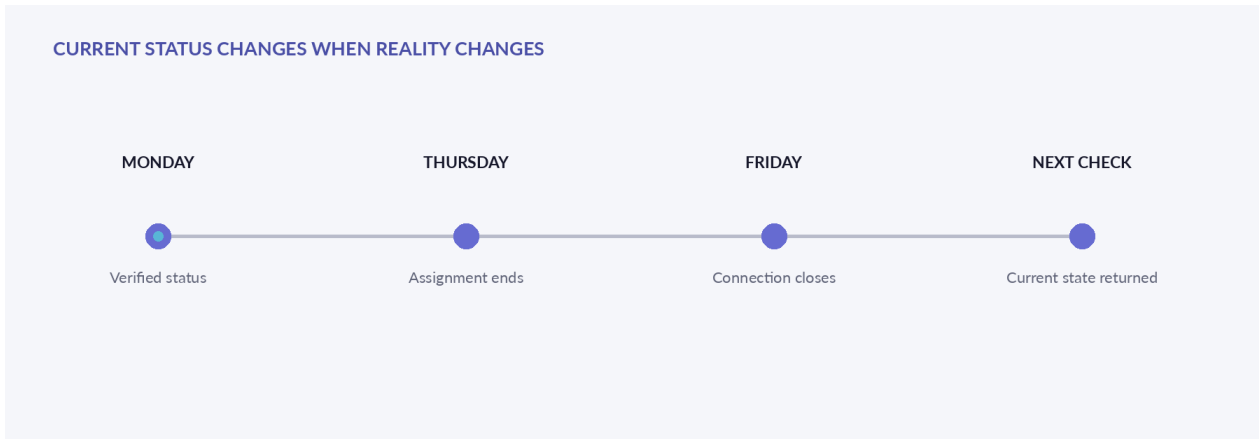
A current status answers:

What is true now?

Both are valuable.

They should not be confused.

Consider a simple timeline.



A PDF created on Monday may still accurately prove Monday.

It does not automatically answer Friday.

That distinction becomes more important as workforce turnover increases.

Point-in-time evidence still matters

Live status does not eliminate the need for historical evidence.

Auditors, clients and incident reviews may need to know:

What did the register show at a particular moment?

A mature evidence model should therefore support both:

Live view

What is current now?

Point-in-time extract

What was the state of the register when this evidence was generated?

The second should be described exactly that way.

It should not be presented as a timeless compliance certificate.

6. A portable credential should point to a live source

A portable credential can make workforce status easier to present across operational environments.

But portability only works if the credential remains connected to current state.

The useful model is:

1. the worker carries a credential reference;
2. the credential is presented;
3. verification resolves against current source status;
4. expiry or revocation changes the verification result;
5. physical identity is still confirmed by the relevant party where required.

This keeps three concepts separate:

- identity confirmation;
- credential presentation;
- readiness status.

A workforce credential can support the second and third.

It does not replace the first.

7. Verification without surveillance

The existence of a readiness requirement does not mean every client needs every piece of worker data.

The operational question is often narrow:

Does this person currently hold the required status?

That question can frequently be answered without exposing:

- detailed assessment scores;
- question-level responses;
- worker rankings;
- full personnel records;
- unnecessary identifiers.

This creates a practical design principle:

verification without surveillance

The authorised view should contain what is needed for the verification purpose.

Programme-management detail can remain inside the appropriate administrative environment.

Status, not scores

Scores can be useful internally when they help programme owners understand assessment quality or learning needs.

But a client-side register does not need to become a ranking system.

The operational state can remain neutral:

- verified;
- not yet verified;
- expired;
- revoked.

This avoids turning readiness evidence into worker profiling.

Low-PII by design

A live register still processes personal data.

The goal should not be "zero PII".

The stronger principle is:

use the minimum personal data needed for the credential and

authorised verification purpose.

This reduces unnecessary data duplication and helps prevent the readiness layer from becoming another personnel database.

8. Identity minimisation is also a security decision

Privacy and identity architecture meet in flexible workforces.

If every client creates a new identity for every external worker, the environment gains:

- more accounts;
- more credentials;
- more lifecycle events;
- more offboarding steps;
- more opportunities for stale identities.

That expands the administrative and technical attack surface.

A workforce register can reduce that pressure by separating:

proof of readiness

from:

client-system identity

where the two do not need to be the same thing.

The worker may still need a client account to perform the job.

The design principle is narrower:

do not create an extra client identity solely because evidence needs somewhere to live.

9. Language is part of evidence integrity

Multilingual delivery is often treated as a usability feature.

In readiness evidence, it can be more fundamental.

If the claim is that the worker understood a required baseline, then the organisation should care whether:

- the language was appropriate;
- translated content preserved meaning;
- assessment routes remained sufficiently equivalent;

- the resulting status means the same thing across language versions.

The important question is not:

How many languages can the interface display?

It is:

Does the resulting status have a consistent meaning across the language routes used to earn it?

That is an evidence-integrity question.

A responsible programme should also distinguish between languages that are:

- live;
- under review;
- planned.

Language claims should reflect actual release status.

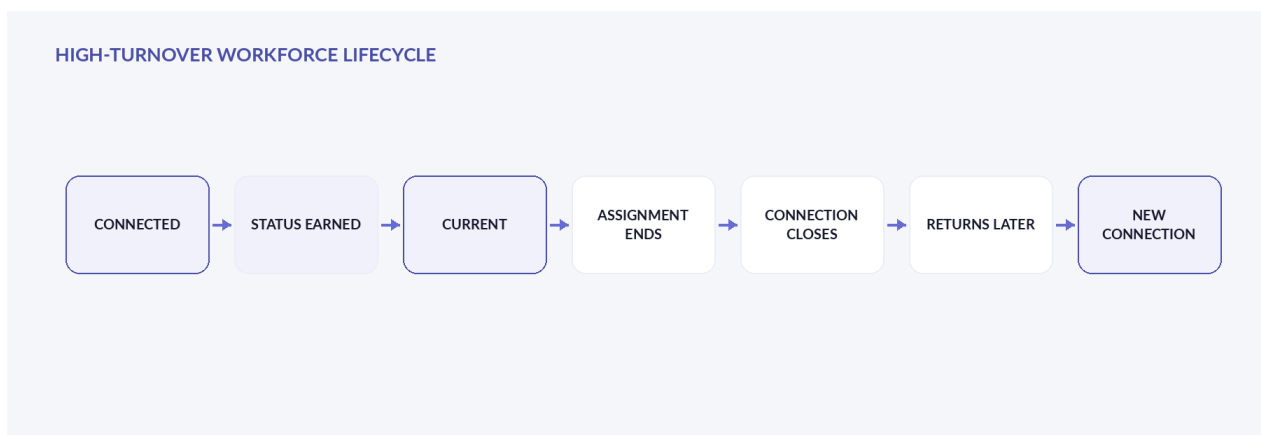
10. High turnover should be treated as normal

Many enterprise systems are optimised for permanent employment.

Flexible labour is different.

People leave and return.

A useful lifecycle looks like this:



The person is not recreated from zero.

The relationship is.

That distinction matters because it lets the system preserve the appropriate worker identity while still treating organisational context as current and explicit.

For staffing agencies and suppliers, this is not an edge case.

It is normal operations.

11. Supplier demonstrability without liability transfer

The Cyberbeveiligingswet's supply-chain focus increases the importance of clear supplier relationships, but it should not be interpreted as automatic liability transfer.

The client remains responsible for its own:

- legal scope;
- risk decisions;
- controls;
- contracting;
- governance.

The supplier's contribution is operational:

maintain accurate, current evidence for the workforce the supplier administers.

A strong supplier evidence model can help answer:

- which workers are relevant;
- which connections are active;
- what status each worker currently holds;
- whether a status is expired or revoked;
- which language route was used where relevant;
- what the register showed at a specific point in time.

That can reduce the client's recurring evidence-collection burden.

It does not make the supplier legally responsible for the client's entire compliance position.

The commercial difference

Compare two client conversations.

Evidence project

Send us an updated spreadsheet and the latest certificates.

Maintained capability

We maintain current workforce status and can make the relevant state demonstrable when you need it.

The second is operationally stronger because it is reusable across client relationships.

12. How this complements GRC, TPRM and security operations

The NIS2 market already has strong systems for governance and technical security.

That is not a problem for a workforce-readiness model.

It clarifies the category.

GRC / ISMS

Useful for:

- requirements;
- controls;
- policies;
- risks;
- evidence ownership;
- corrective actions.

Third-party risk management

Useful for:

- supplier inventories;
- supplier assessments;
- risk classification;
- contract controls;
- recurring review.

SOC / MDR

Useful for:

- telemetry;
- detection;
- incidents;
- technical monitoring;
- response.

Workforce readiness

Useful for:

- people;
- current organisational connections;
- current workforce status;
- verification;
- lifecycle across assignments.

The architecture should be composable.

Where useful, workforce evidence can flow into the wider governance environment.

The specialist layer does not need to become the system for everything.

13. A practical checklist for operators

Organisations using multiple suppliers can start with a small set of questions.

Workforce boundary

- Have we identified the external worker populations relevant to cyber risk?
- Do we know which supplier administers each population?
- Do we know when those relationships start and end?

Requirement

- Is the expected readiness status defined?
- Does it reflect role and risk?
- Is the requirement different for different populations where necessary?

Status

- Can we distinguish current status from historical activity?
- Can status expire?
- Can it be revoked?
- Can it be revalidated?

Verification

- Can an authorised party verify the current state?
- Are we still dependent on manually reconstructed spreadsheets?

Data

- Are we collecting only what the verification purpose needs?
- Are we duplicating worker identities unnecessarily?

Language

- Can relevant workers use an appropriate language route?
- Is language equivalence treated as part of evidence quality?

Supplier relationship

- Is the supplier expected to maintain the evidence?
- Are responsibilities clear?
- Can evidence be reused across the relationship rather than rebuilt repeatedly?

14. A practical checklist for staffing agencies and workforce suppliers

Client demand

- Which clients already ask workforce-security questions?
- Which clients are strengthening cybersecurity clauses?
- Are the same questions appearing repeatedly?

Population

- Which workers are currently connected?
- Which are active at which client or site?
- Who has left?
- Who has returned?

Status

- Which workers currently hold the required status?
- Which are not yet verified?
- Which have expired?

- Which have been revoked?

Evidence

- Are we relying on static files?
- Can an authorised client verify status directly where appropriate?
- Can we generate point-in-time evidence when needed?

Identity

- Are clients creating extra accounts solely to carry evidence?
- Can readiness be demonstrated without another full personnel record?

Language

- Are the relevant language routes actually live?
- Does the status mean the same thing across those routes?

Commercial reuse

- Can the same readiness capability support more than one client relationship?
- Does sharing create unnecessary duplicate cost?
- Does the worker remain free?

A reusable register capability is more durable than a one-client evidence project.

15. The EdXactly model

EdXactly is designed as a **live register of workforce cyber readiness**.

The product model separates the layers deliberately.

Connection

A worker is connected to the relevant organisational relationship.

The connection is the context in which readiness matters.

Readiness pathway

Training and assessment can be included in the connection and are how the worker earns the required status.

They support the register.

They are not the category EdXactly is trying to create.

Current status

The operational result is a current status:

- verified;
- not yet verified;
- expired;
- revoked.

The register does not need to expose a worker score to answer the client-side status question.

EdXactly Pass

The worker can carry a portable credential linked to the live register status.

The credential is useful because verification resolves against current state rather than relying on a static image alone.

EdXactly Switch

A client can consolidate connected supplier workforce status in one register view.

This supports supplier demonstrability without turning the client into the owner of every supplier's internal worker record.

EdXactly Flex

Where the physical site is the relevant commercial unit, EdXactly Flex provides direct site-level workforce coverage.

16. The commercial principle

EdXactly's commercial model is designed to reinforce the infrastructure model.

You pay for register capacity and connections, never per training. Training and assessment are included in every connection; they are how a name earns its place in the register.

Workers remain free.

Verification is never charged twice.

The aim is to make readiness evidence reusable across the labour relationship rather than repeatedly monetising the same worker activity.

17. What EdXactly does not claim

EdXactly does not:

- determine whether a particular organisation is in scope of the Cyberbeveiligingswet;
- determine which workforce populations an organisation must include;
- certify legal compliance;
- replace a risk assessment;
- replace technical cybersecurity controls;
- replace an ISMS, GRC platform or SOC;
- transfer legal liability between client and supplier;
- treat a not-yet-verified worker as inherently unsafe;
- replace physical identity confirmation where that is required;
- turn a historical record into a timeless certificate.

The register is an evidence and verification layer.

It supports demonstrability.

That boundary is part of the product's credibility.

18. Conclusion

NIS2 and the Cyberbeveiligingswet make supply-chain cybersecurity more operational.

For many organisations, the next gap will not be another policy or framework.

It will be maintaining a current answer about the people moving through those frameworks.

The workforce evidence problem can be reduced to seven questions:

**Who is relevant? Which connection is active? What is required?
What is the current status? Is it still valid? Can it be verified?
What happens when the person leaves and returns?**

When those answers live in separate spreadsheets, client systems and historical certificates, the evidence becomes expensive to maintain and easy to age.

A live workforce register creates a different operating model.

It keeps readiness attached to the active relationship.

It lets current status change when reality changes.

It supports point-in-time evidence without pretending that old evidence is forever current.

And it gives suppliers and clients a clearer way to share demonstrability without duplicating every worker into every system.

That is the role of the workforce-readiness layer.

The live register of workforce cyber readiness.

Sources and further reading

All regulatory references were reviewed on 14 September 2026.

[1] Rijksoverheid - Cyberbeveiligingswet and Wwke in force

15 August 2026 Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf vandaag van kracht

<https://www.rijksoverheid.nl/actueel/nieuws/2026/08/15/cyberbeveiligingswet-en-wet-weerbaarheid-kritieke-entiteiten-vanaf-vandaag-van-kracht>

[2] Nationaal Cyber Security Centrum - Cbw duty of care

NCSC's current guidance sets out the ten duty-of-care measures, including supply-chain security, cyber hygiene/security training, personnel/access/asset security and effectiveness assessment.

<https://www.ncsc.nl/cyberbeveiligingswet-nis2/zorgplicht>

[3] Directive (EU) 2022/2555 - NIS2

EUR-Lex

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>

[4] Nationaal Cyber Security Centrum - Suppliers of Cbw organisations

Current NCSC guidance on how Cbw organisations may impose cybersecurity requirements on direct suppliers/service providers where the supply relationship creates relevant network and information-system risk.

<https://www.ncsc.nl/cyberbeveiligingswet-nis2/toeleveranciers-van-cbw-organisaties>

[5] Nationaal Cyber Security Centrum - Safe digital behaviour

NCSC guidance emphasising that knowledge alone is insufficient and that organisations should diagnose, measure and support safe digital behaviour rather than treating a mandatory e-learning as the complete solution.

<https://www.ncsc.nl/mensgerichte-beveiliging/hoe-bevorder-je-veilig-digitaal-gedrag-van-medewerkers>

[6] Nationaal Cyber Security Centrum - Five basic principles

Basisprincipe 2: Bevorder veilig gedrag

<https://www.ncsc.nl/basisprincipes/basisprincipe-2-bevorder-veilig-gedrag>

[7] ENISA - NIS2 Technical Implementation Guidance

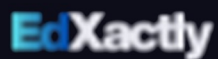
Published 26 June 2025. The guidance supports the NIS2 Implementing Regulation for specified digital infrastructure, ICT service-management and digital-provider categories and should not be treated as a universal implementation guide for every NIS2 entity.

<https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance>

Editorial metadata

Published: 14 September 2026 **Last reviewed:** 14 September 2026 **Jurisdiction:** Netherlands / EU NIS2 **Primary official sources:** Rijksoverheid, NCSC, EUR-Lex, ENISA

Document status: General information, not legal advice.

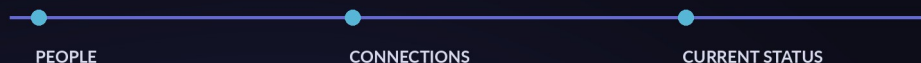


THE LIVE REGISTER OF

WORKFORCE CYBER READINESS

EdXactly connects people, organisational relationships and current workforce status in one verification layer.

Training and assessment can sit inside the connection; the register keeps the operational status current and shareable where authorised.



Explore the platform

edxactly.com

EdXactly V.O.F. · KVK 99557487 · Heeze, Netherlands