ComplyAssist

Getting Started Guide

From first setup to your first checklist. A practical guide to getting started with confidence.

GlobalConnect

Getting started

The purpose of this manual is to help you get started with ComplyAssist, the practical tool designed for those responsible for getting compliance work done.

If ComplyAssist is not performing as expected or you encounter critical issues, reach out to our support immediately. We are ready to help you troubleshoot and get your compliance journey back on track.

GlobalConnect Support
075-100 00 00
customersupport@globalconnect.se

GlobalConnect

Version number: 1.0
Responsible editor: CLC team

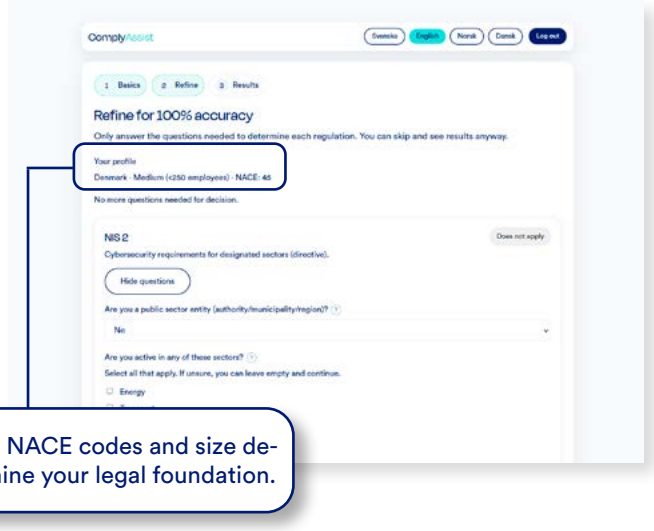
Table of Content

Step 1: Create Your Organization/ business Profile

The Onboarding Wizard is your scope engine. It uses basic business facts to identify which EU regulations (like NIS2, GDPR, or DORA) likely apply to you.

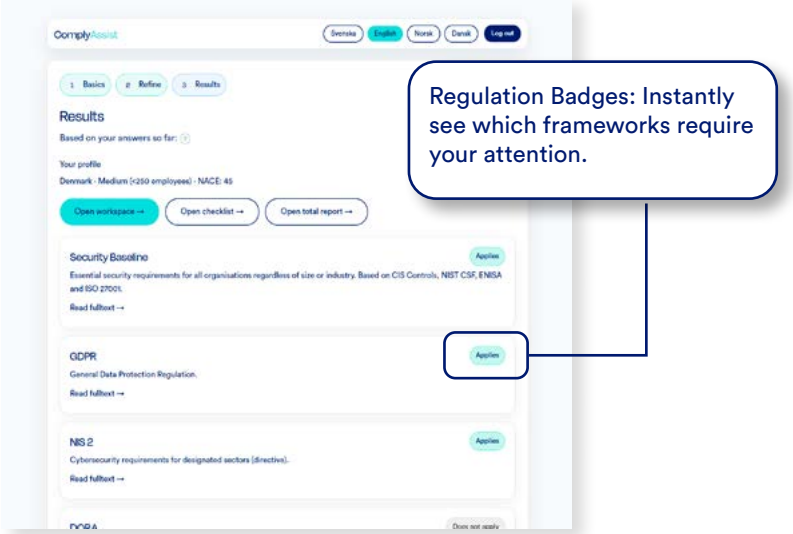
1 Start by entering your country, company size, and NACE (industry) codes.

Figure 1: The Onboarding Wizard – Scoping with Business Facts



2 Answer the highlighted follow-up questions. If you are unsure, select “Don’t know” rather than guessing; you can refine this later.

Figure 2: Regulation Results – Identifying Applicable Frameworks



3 Review your results. You will see badges marking frameworks as “Applies,” “Indirect,” or “Does not apply”.

What if you want to edit some of your initial onboarding choices

If you need to update your core organization profile, such as changing your country, company size (number of employees), or NACE codes, simply click ‘Your journey’ in the top navigation bar and choose “Profile”. Go to the bottom and choose “Back”.

Please be aware that changing these foundational facts will reset your previous follow-up answers; this is a safety feature to ensure your legal scope remains accurate based on your new profile.

If you only wish to revise your specific regulation responses without changing your company size or sector, use the ‘Edit answers’ button on the results page instead to return to the refinement step.

Did you know!

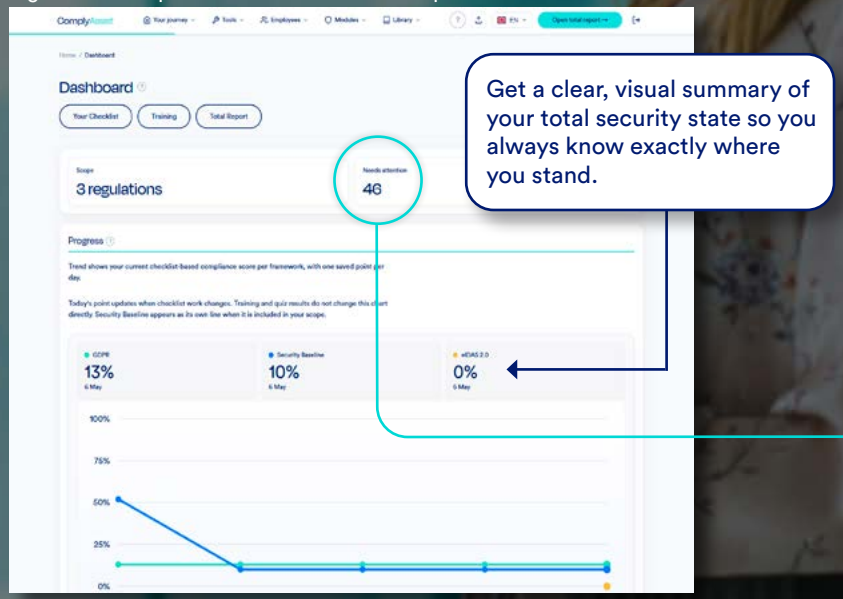
ComplyAssist is designed for the people who “run the work,” not just legal specialists. You never need to start with complex legal texts. By starting with simple business questions, the system translates law into a practical, operational workflow for you.

Step 2: Navigate Your Operational Cockpit (The Dashboard)

Once your profile is set, the Dashboard becomes your daily starting point to prioritize work.

1. Check your Compliance Score trend. This weighted percentage shows your progress over time.

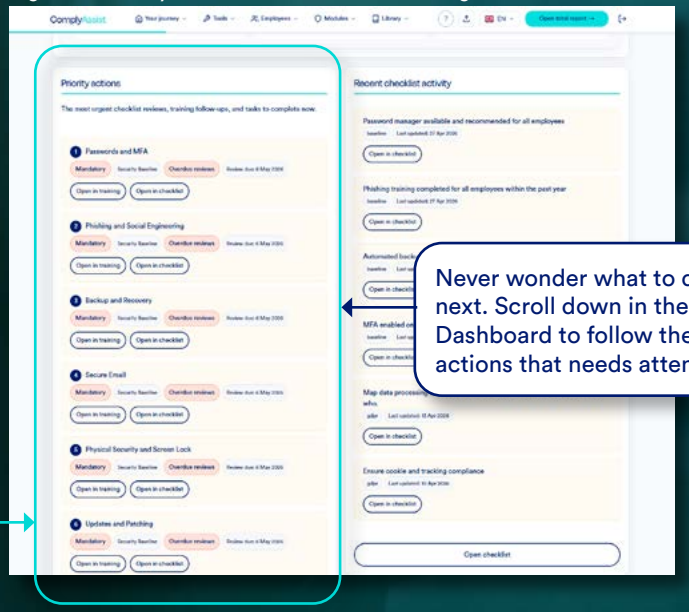
Figure 3: The Operational Dashboard – Compliance Score & Trend



2. Identify “Priority Actions.” Focus on the Top 5 most urgent items, such as overdue reviews or expired training.

3. Monitor recent activity. See what has changed recently to ensure you and/or your team is moving in the right direction.

Figure 4: Priority Actions – Focused Task Management

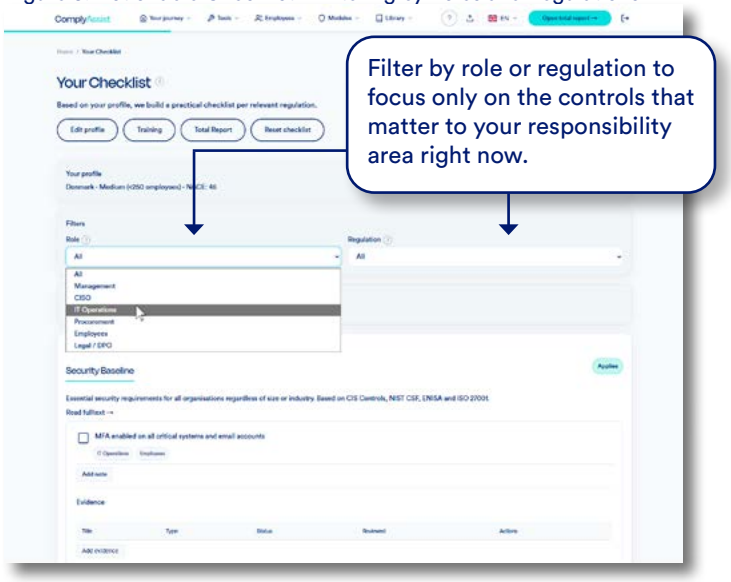


Step 3: Execute in the Actionable Checklist

The Checklist is where compliance becomes operational work.

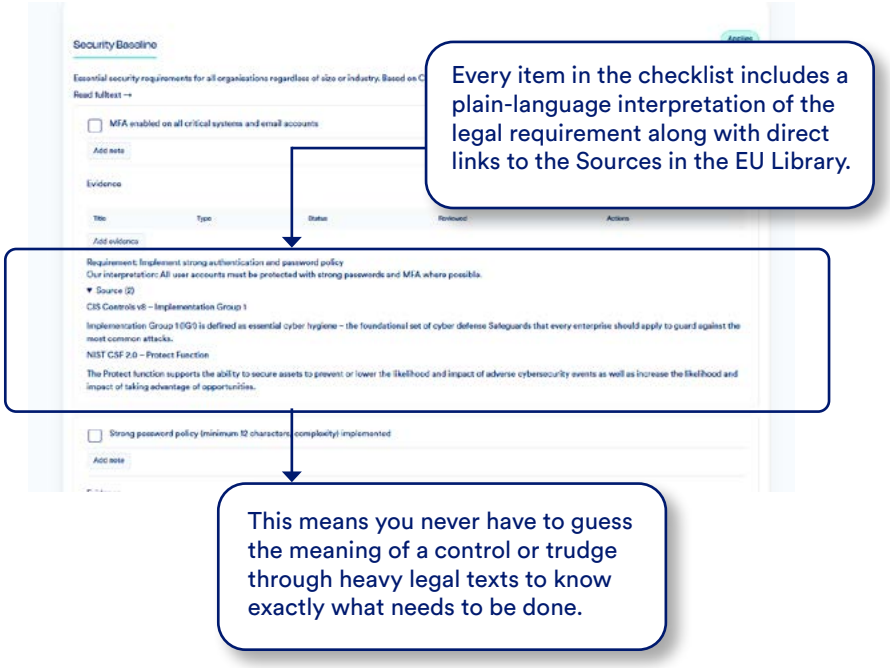
1. Start narrow. Filter by a specific Role (e.g., IT Operations or Legal) or Regulation to avoid feeling overwhelmed.

Figure 5: Actionable Checklist – Filtering by Roles and Regulations



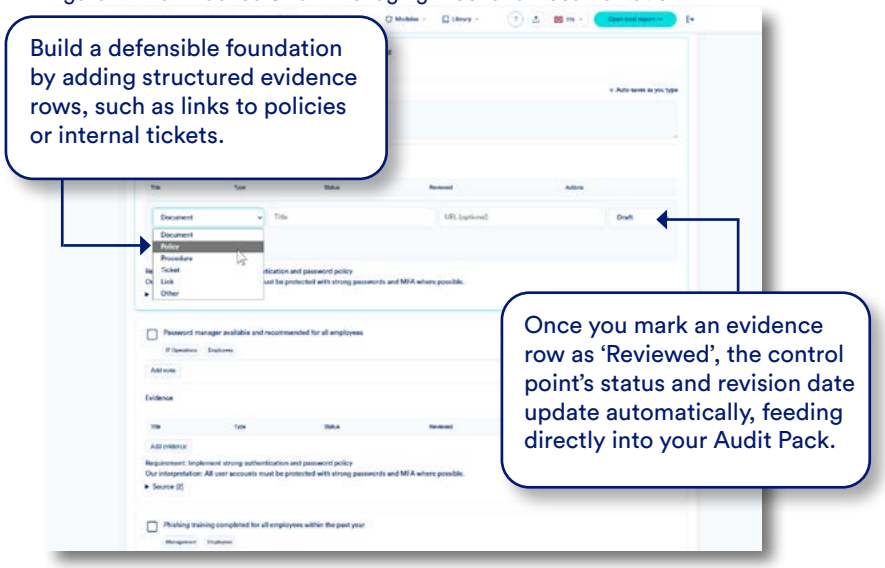
2. Read the context. Use the requirement summary and sources to understand the goal of each control.

Figure 6: Control Context – Requirements and Source Links



3. Add factual notes. A “done” checkbox is weak proof. Write short, factual notes explaining where the evidence is or who approved the action. See figure 7 below.

Figure 7: The Evidence Grid – Managing Proof and Documentation



4 Attach structured evidence. Add rows for policies or links and mark them as "Reviewed" to update your maturity level.

Evidence standard

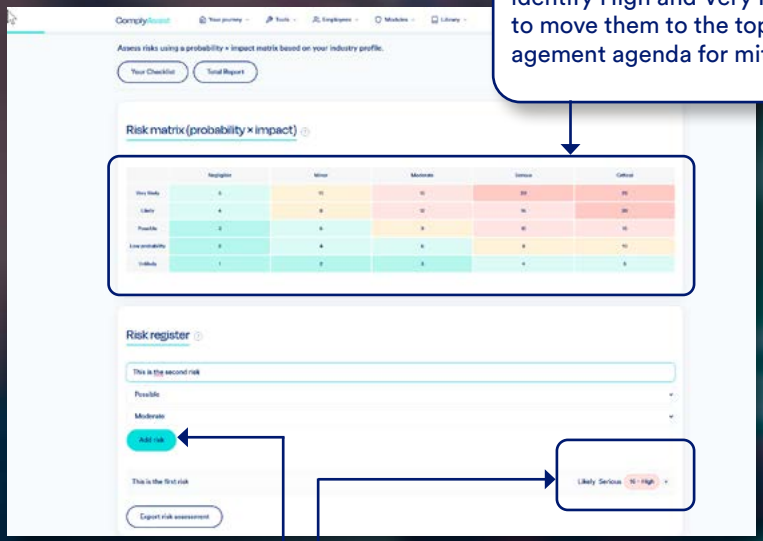
Show, don't just tell! Real confidence comes from being able to show what was done, when, and by whom. Use the Evidence Grid for structured proof (like policies or tickets) and the Notes field to provide the necessary organizational context. A simple "done" is never enough for an auditor.

Step 4: Use Specialist Tools (Risk & Training)

Use standalone modules for specific tasks that support your checklist work.

1 The Risk Calculator: Quickly rank threats by probability and impact.

Figure 8: Risk Matrix – Visualizing Probability



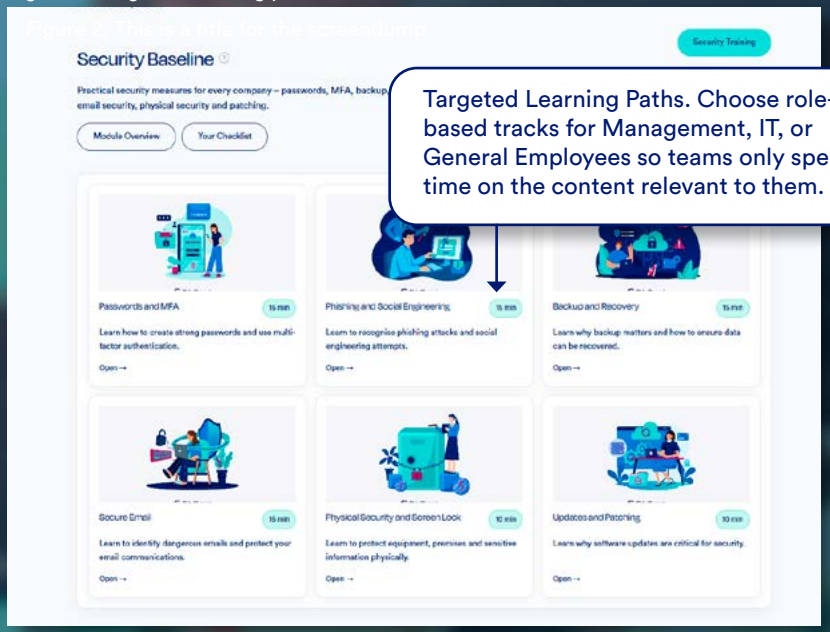
Operational Heatmap". Instantly identify High and Very High threats to move them to the top of your management agenda for mitigation.

"Event-Based Scoring" – Define concrete events (e.g., "Ransomware on file server") and score them from 1–5 on probability and impact to get a rank between 1 and 25.

2 The Training Module: Roll out role-based security awareness quizzes to staff.

This module transforms security awareness into a shared organizational responsibility with role-based tracks.

Figure 9: Targeted learning paths



Targeted Learning Paths. Choose role-based tracks for Management, IT, or General Employees so teams only spend time on the content relevant to them.

Opening a track gives you a possibility to share the track with your colleagues or employees. See figure 10.

Figure 10 : Training Module – Role-Based Awareness Tracks

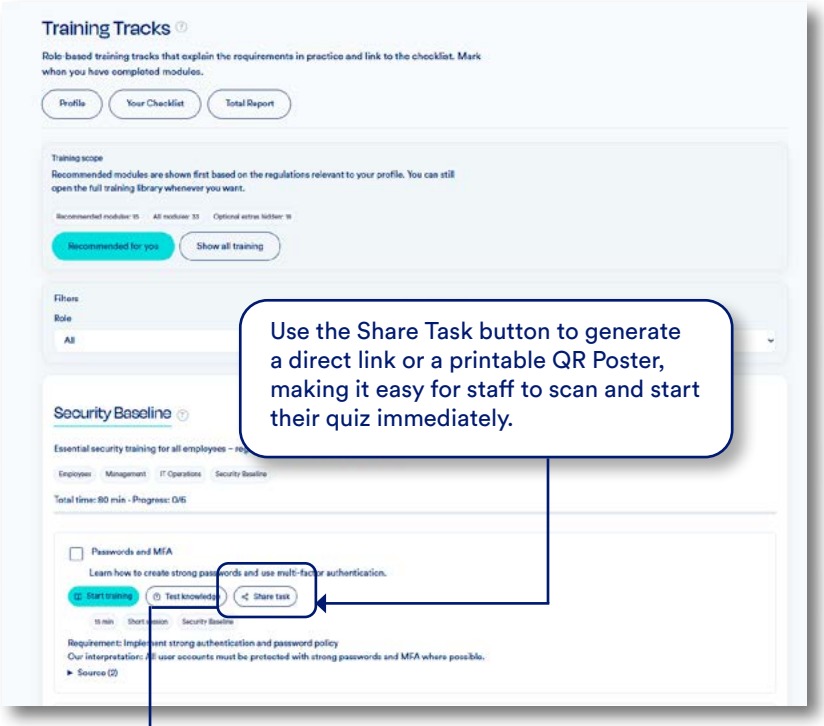


Figure 11: Share Task Modal – QR Codes and Invite Links

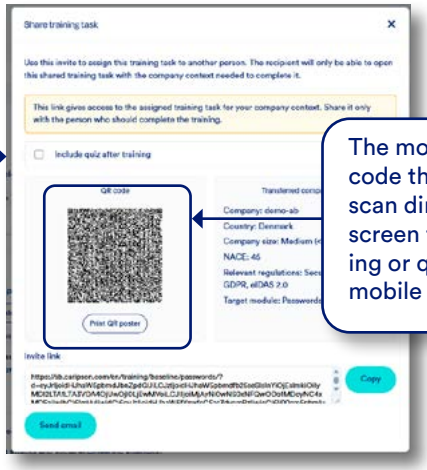
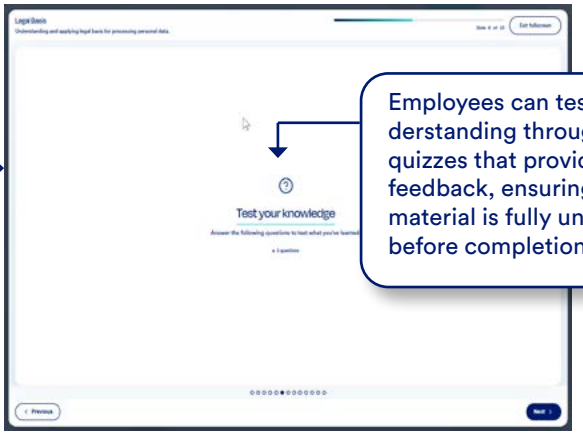
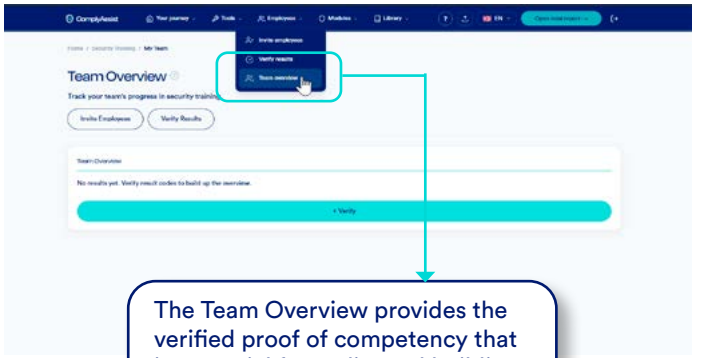


Figure 12: Interactive Quiz – Employee Knowledge Testing



You can track employee progress by clicking ‘Team Overview’ in the navigation bar to see a live status of completed modules, pass rates, and individual performance.

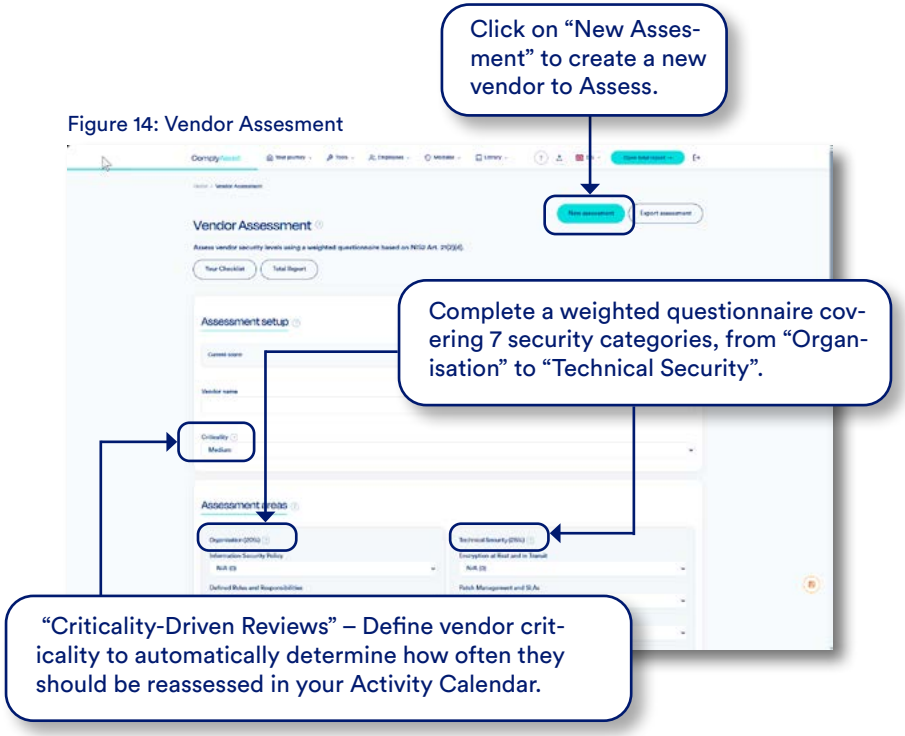
Figure 13: Team Overview – Tracking Staff Progress



3 The Vendor Assessment: Your security is only as strong as your weakest supplier.

Use the tool “Vendor Assessment” to evaluate them in a structured way by scoring them based on their security posture.

Figure 14: Vendor Assesment

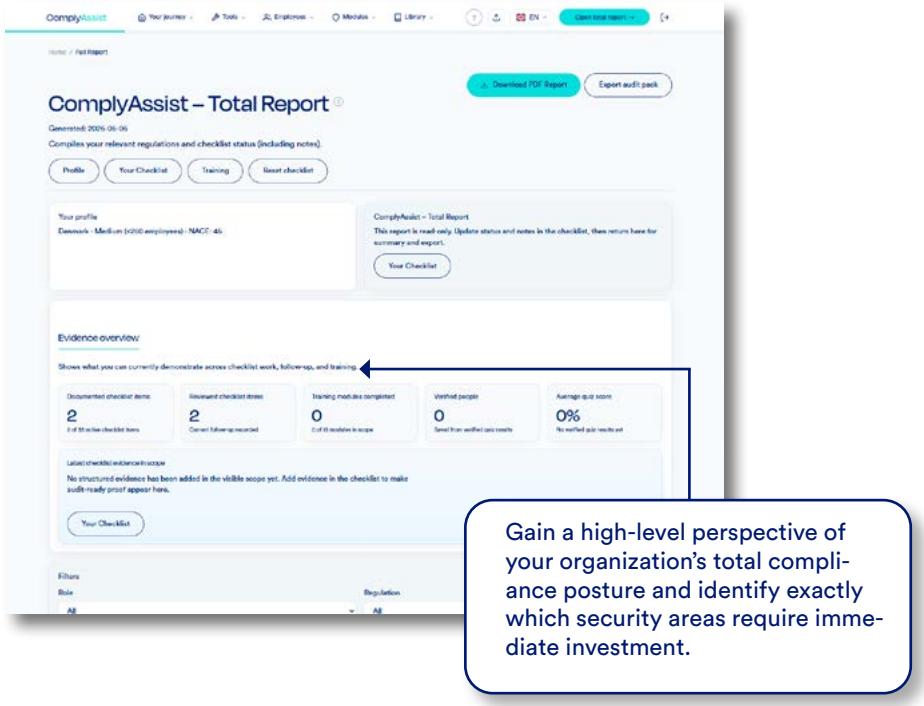


Step 5: Review and Export

When management, auditors or other stakeolders need proof, move to the Report page. You can find it in the menu under “Your journey”. It is called “Total report”.

1. Review the Executive Summary. This provides a plain-language status for management discussion.

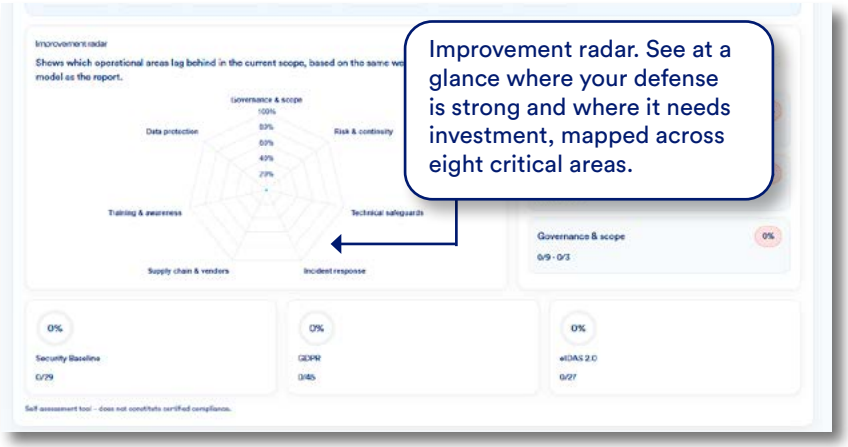
Figure 15: The Total Report – Executive Summary and KPIs



Gain a high-level perspective of your organization’s total compliance posture and identify exactly which security areas require immediate investment.

2. Check the Improvement Radar further down the page. Here you can visualize your strengths across areas like Governance and Technical Safeguards.

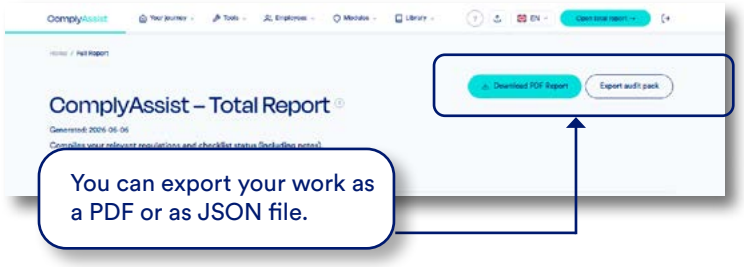
Figure 16: Improvement Radar – Visual Gap Analysis



Improvement radar. See at a glance where your defense is strong and where it needs investment, mapped across eight critical areas.

3 The report page offers two distinct ways to export and share your progress. They are designed for different audiences and serves different purposes:

Figure 15: Export Menu – PDF Snapshots vs. Audit Packs



- **Download PDF Report (The Snapshot):** This is a browser-generated snapshot of your current report view. It is best for management briefings, steering meetings, and quick status snapshots. It provides a polished, “board-friendly” presentation of your scores, action plan, and checklist status.

- **Export Audit Pack (The Deep-Dive):** This is a structured JSON file (see the info box below) designed for technical transparency and traceability. It is best for professional auditors and large B2B customers who need to verify your work. Unlike the PDF, the Audit Pack contains your full activity history, evidence links, timestamps, and integrity hashes, providing the deep-dive proof required for formal audits.

Pro Tip: Use the PDF to show where you are, and use the Audit Pack to prove how you got there.

What is a JSON file, and why does it matter?

Most people are familiar with PDFs, which are “human-readable” snapshots, essentially a digital printout. A JSON file (JavaScript Object Notation), however, is a “machine-readable” format.

Who uses it? You don’t need to read the JSON file yourself. It is designed for professional auditors and technical teams.

Why is it important? While a PDF shows where you are, the JSON Audit Pack proves how you got there. It contains every timestamp, note, and “integrity hash” (a digital fingerprint) that proves your documentation hasn’t been tampered with.

If an auditor needs to verify your full compliance history, the JSON file is the only evidence that provides total traceability.

Step 6: Secure Your Data (Backup & Restore)

ComplyAssist is built on a “privacy-first” architecture, meaning all your working data, checklists, notes, and evidence, is stored locally in your browser rather than on a central cloud server.

This gives you full ownership of your data, but it also means that you are responsible for its preservation.

Follow these three steps to ensure your work is never lost:

1. Make backup a routine. Export an encrypted .gcbak file regularly.

   Because your workspace lives only in your browser’s local storage, your data will be permanently deleted if you clear your browser’s cookies or local data.

To prevent this, treat exporting as a core operational task:

- **How**: Click on the Save icon bottom right on any page.
- **When:** We recommend exporting a fresh copy after every major work session.

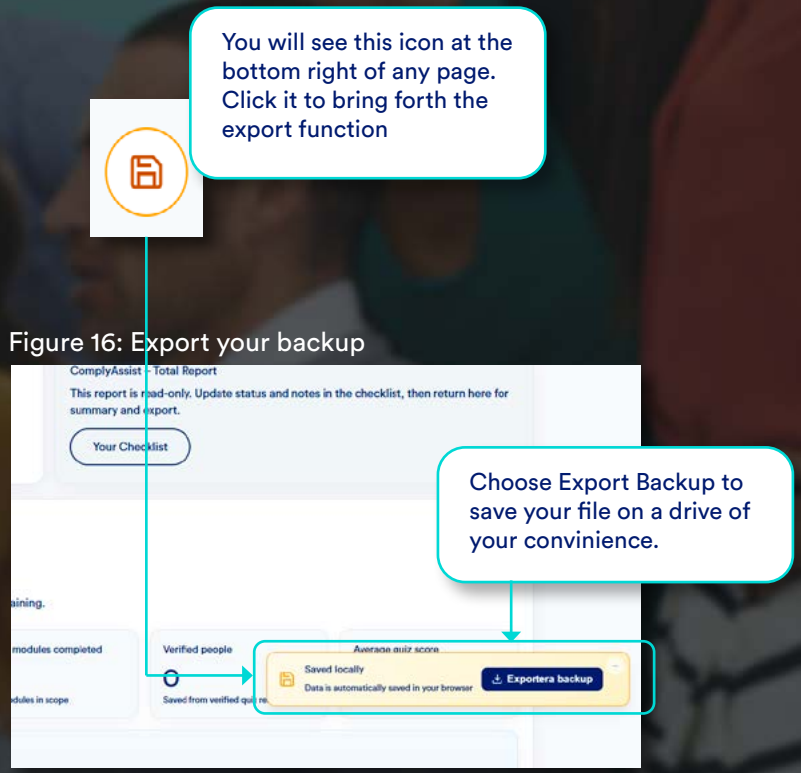
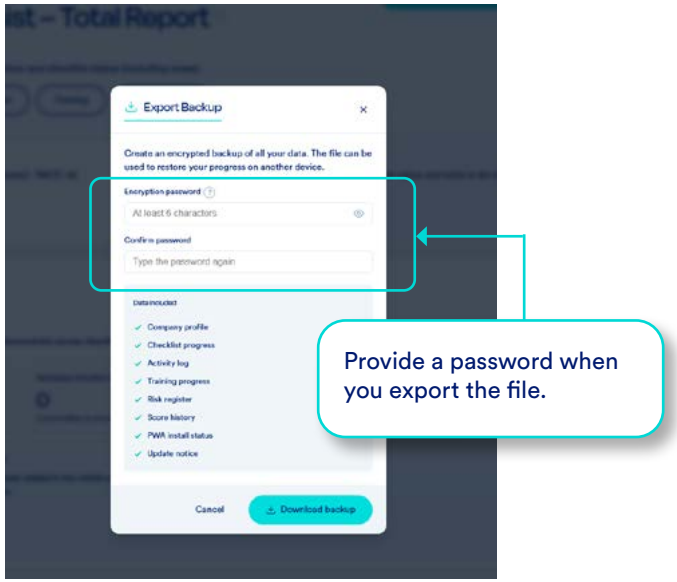


Figure 16: Export your backup

2 Use a strong password. When you export a backup, the system asks you to provide a password.

This password is used to encrypt your file using the AES-256 standard.

Figure 17: Export Backup – Secure Passwords



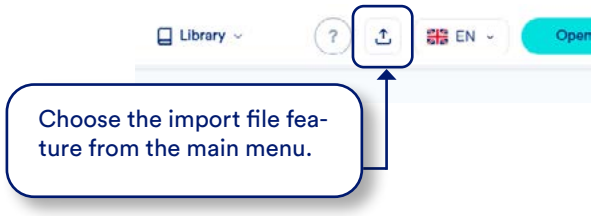
- **The "Key" to your data:** Your password acts as the unique encryption key. Without it, the .gcbak file is just unreadable text that cannot be opened by anyone else.

- **No recovery options:** Because GlobalConnect does not store your data or your passwords, there is no "forgot password" function. If you lose this password, the data inside the backup file can never be recovered. Always store your backup password securely for instance in a corporate password manager.

3 Import to switch devices. To move your work to a new computer or a different browser, you must manually move your data using your backup file.

- **How:** On your new device, select "Import a backup" from the welcome screen or the main menu and upload your latest .gcbak file.

Figure 18: Import Backup – Restoring Your Workspace



- **Data Replacement:** Be aware that importing is a “replace” action, not a merge. The imported file will overwrite any existing ComplyAssist data currently in that browser.

- **Activate Access:** Remember that while the backup restores your work, you still need to enter your license token to unlock the platform’s features on the new device.

Important! Privacy-First: Your Data, Your Ownership

ComplyAssist uses a “privacy-first” architecture where your data is stored locally in your browser, not on a central cloud server. This gives you full ownership but also means you are responsible for your own backups. **Always export a .gcbak file before clearing browser data or switching devices.**

Not Directly Regulated? Why ComplyAssist Still Matters

Even if your organization does not currently fall under EU regulations such as NIS2 or DORA, practical security is no longer optional.

ComplyAssist helps businesses move from ad-hoc IT practices to a structured and manageable security approach. It creates a repeatable foundation that strengthens resilience, protects your data, and supports your reputation, regardless of regulatory status.

Trust as a Competitive Advantage

In today's digital landscape, professional trust is your most valuable asset. Even if your organization is not directly regulated by EU mandates like NIS2 or DORA, your partners, board members, and customers certainly are.

Providing transparent documentation of your security routines creates a significant competitive edge, turning your commitment to safety into a key reason for others to choose you.

Here are some reasons why you should use ComplyAssist even though you do not fall under the scope of the various regulations:

1. Use your **Compliance Score** and **Audit Pack** as professional proof to build instant trust during procurement, sales cycles, or when applying for insurance.

2. Replace "tribal knowledge" and memory with a documented system that survives staff turnover and ensures consistency in your daily operations.

3. Regulations are constantly expanding. Starting with a solid baseline ensures that as your business grows or new requirements appear, you are already prepared and halfway to full compliance.

Security as a Business Enabler

Even if you aren't directly regulated by NIS2 or DORA, your customers likely are. Being able to document your security posture through the Security Baseline provides a significant competitive advantage, building instant trust and making it easier to win new business.

Want to watch videos on how to use ComplyAssist?

Want to know more about ComplyAssist or watch our how-to videos.

Learn more by pointing your smartdevice towards the QR code below.

GlobalConnect is operating and supporting more than half of all data traffic in the Nordics

We are

Delivering fiberbased Broadband services to more than 30.000 businesses

One of the leading operators of digital infrastructure in Northern Europe

Employing about 2000 employees across the Nordic Countries

Owner of more than 35.000 m^2 of modern, highly secure green datacenters.

The proud owner of more than 250.000 km of fibernetwork

A provider of highly efficient cyberprotection and cloudbased backup services.

GlobalConnect

Contact us to hear more