CB

ComplianceBridge

CISO Quick-Start Guide

Stop doing compliance twice.

VERSION 1.0 · MARCH 2026

What's Inside

1	**Dashboard**	Your compliance command center
2	**Framework Mapping & Gap Analysis**	Know what you already have
3	**Compliance Status Tracker**	Track implementation control-by-control
4	**Incident Reporting Orchestrator**	6 regulators, one workflow
5	**Policy Template Library**	One policy set, both jurisdictions
6	**Recommended First-Week Workflow**	Day-by-day onboarding playbook
7	**Framework & Deadline Reference**	Quick-reference tables

6	76	70+
FRAMEWORKS	CONTROLS	CROSS-MAPPINGS

1 Dashboard

Your compliance command center — a single screen that tells you where you stand across both jurisdictions.

The moment you open ComplianceBridge, the dashboard gives you an instant read on your dual-jurisdiction posture. No clicking through menus, no loading reports. Just the numbers that matter.

📊

Stats at a Glance

Total frameworks, controls mapped, and a split by jurisdiction. You see it before you scroll.

⚡

Quick Actions

One-click cards to jump into Mapping, Compliance, Incidents, or Policies.

📡

Regulatory Feed

Curated updates color-coded by impact: critical, high, medium, low. Know what's moving before your auditor does.

🏛️

Framework Overview

All 6 frameworks with control counts, versions, and effective dates. Israel in blue, USA in red.

CISO TIP

Check the regulatory feed weekly. A single update — like CMMC enforcement going live or a new INCD directive — can change your compliance posture overnight. The feed tells you what changed, who's affected, and what action to take.

---

2 Framework Mapping & Gap Analysis

This is the feature that saves you the most time. Instead of hiring consultants to manually map Amendment 13 controls to NIST CSF, ComplianceBridge does it instantly.

How to use it

1. **Select your source framework** — the one you already comply with (e.g., "NIST CSF 2.0")
2. **Select your target framework** — the one you need to comply with (e.g., "Amendment 13")
3. The platform runs **two analyses simultaneously** under the Gap Analysis and Control Mapping tabs

Gap Analysis Tab (Default)

Shows you a **coverage percentage** — the share of target controls already satisfied by your source framework. Below that:

- **Covered controls** — controls you can check off immediately, with the exact source control that satisfies each one
- **Gap controls** — the incremental work. Controls in the target framework with no equivalent in your source

"We're 72% covered for Amendment 13 based on our existing NIST CSF posture. Here are the 9 gaps."

That's your board slide.

Control Mapping Tab

A detailed, searchable table of every control-to-control relationship. Each row shows:

COLUMN	WHAT IT TELLS YOU
Source → Target	Control codes and titles for both sides of the mapping
Mapping Type	`equivalent` direct match `partial` covers some `related` thematically similar
Confidence	Visual bar showing mapping strength (0–100%)
Rationale	Click any row for a detailed explanation of why these controls map

CISO TIP

Run gap analyses in **both directions**. "NIST CSF → Amendment 13" tells you what you need for Israel. "Amendment 13 → SOC 2" tells you what your Israeli compliance already gives you toward your US audit. Present both to leadership — it shows ROI on compliance work.

3 Compliance Status Tracker

Once you know your gaps, you need to close them. The tracker takes every control through its lifecycle: Not Started → In Progress → Implemented → Verified.

How to use it

1. **Select a framework** from the dropdown (grouped by jurisdiction — Israel / USA with colored indicators)
2. Review the **summary cards**: completion percentage, status counts, and a visual progress bar
3. **Search and filter** the control table — filter by status to focus your team's work
4. Click **"Update"** on any control to change its status, add evidence notes, and view implementation guidance

Status Lifecycle

STATUS	MEANING	WHO SETS IT
Not Started	Control hasn't been addressed yet	Default
In Progress	Implementation work is underway	Control owner
Implemented	Control has been put in place	Control owner
Verified	Independently validated by audit or review	Internal audit / third party

CISO TIP

Reserve "Verified" for controls that have been independently validated. This creates a clear audit trail: implemented first, then verified. Auditors love this distinction — it shows rigor in your compliance process.

4 Incident Reporting Orchestrator

When an incident hits, your team shouldn't be scrambling through spreadsheets to figure out who to call. ComplianceBridge calculates every obligation automatically.

Reporting a New Incident

The intake form captures everything needed to determine your regulatory obligations:

FIELD	WHY IT MATTERS
Title & Description	Internal tracking and report template pre-fill
Incident Type	Data breach, ransomware, unauthorized access, etc. — determines which regulations trigger
Severity	Critical / High / Medium / Low — affects prioritization and some thresholds
Discovery Date	All regulatory clocks start from this moment
Jurisdictions	Check Israel, USA, or both — the key trigger for obligation calculation

The Four Critical Checkboxes

These characteristics determine exactly which regulators you must notify:

CHARACTERISTIC	TRIGGERS
Personal data involved	Israel PPA (72h), California AG (72h), NY AG/DFS (72h)
Critical infrastructure	INCD mandatory reporting (6h)
Material financial impact	SEC 8-K filing (96h / 4 business days)
Controlled Unclassified Info (CUI)	DIBCAC (72h), CIRCIA (72h)

What You Get Back

After submission, ComplianceBridge presents a **timeline view** of every obligation, sorted by urgency:

- Regulator name and legal basis
- Exact deadline (date + time) calculated from your discovery date
- Time remaining with color-coded urgency
- Status tracking: pending → submitted → acknowledged

Managing Ongoing Incidents

The **History tab** shows all reported incidents with severity badges, jurisdiction tags, and obligation counts. Click any incident to update its status (Open → Investigating → Contained → Resolved → Closed) and mark individual obligations as filed.

> **CISO TIP**
>
> Run a tabletop exercise. Enter a hypothetical "ransomware attack affecting personal data of Israeli and US customers, critical infrastructure involved." Watch every obligation light up. Use the output as your incident response playbook. Your IR team should know these deadlines *cold* before an incident happens — not during one.

---

5 Policy Template Library

Maintaining separate policy sets for Israel and the US is a waste of your team's time. ComplianceBridge provides dual-jurisdiction templates that satisfy both simultaneously.

10 Core Templates

POLICY	COVERAGE
Information Security	Overarching security program — NIST CSF, Amendment 13, SOC 2
Data Protection & Privacy	Israel PPA, CCPA/CPRA, Amendment 13 privacy requirements
Incident Response	Multi-jurisdiction IR plan with both countries' reporting procedures
Access Control	Identity & auth — NIST AC family, Amendment 13, SOC 2
Acceptable Use	Employee security responsibilities across both jurisdictions
Data Retention	Retention schedules compliant with Israeli and US law
Vendor Risk Management	Amendment 13 supplier requirements, SOC 2 vendor controls
Business Continuity / DR	Recovery objectives, backup, continuity planning
Encryption & Key Management	Crypto standards, key lifecycle, transport security
Change Management	Change control processes for regulated environments

Each template includes **jurisdiction badges** showing which countries it covers, **framework tags** for specific regulation references, and **inline regulatory annotations** marking which sections satisfy which requirements.

Templates can be **copied to clipboard** or **downloaded as Markdown** for import into your document management system.

CISO TIP

Don't adopt these templates wholesale. Use them as a baseline. The regulatory annotations are the real value — they tell you exactly which sections are load-bearing for compliance, so you know what you can customize and what you shouldn't touch.

6 Recommended First-Week Workflow

A day-by-day onboarding playbook to get maximum value from ComplianceBridge in your first five days.

DAY 1 — UNDERSTAND YOUR POSTURE

Baseline assessment

Open the Dashboard. Review supported frameworks and recent regulatory updates. Go to Framework Mapping and run gap analyses between every framework pair relevant to your organization. Screenshot the coverage percentages — this is your baseline.

DAY 2–3 — SET UP TRACKING

Honest status assessment

Open the Compliance Tracker. Select your primary framework and walk through each control. Set honest statuses — mark what's truly "Implemented" vs. what's aspirational. Repeat for your secondary framework. You now have a real compliance posture, not a guess.

DAY 4 — PREPARE FOR INCIDENTS

Tabletop exercise

Open the Incident Reporter and run a tabletop exercise with your IR team. Submit a realistic hypothetical incident affecting both jurisdictions. Review every obligation that triggers. Ensure your team knows the deadlines.

DAY 5 — POLICY BASELINE

Gap identification

Open the Policy Library and review each template against your existing policies. Identify gaps: which do you have, which are missing, which cover only one jurisdiction? Download templates for missing policies and begin customization.

ONGOING

Sustaining cadence

Weekly: Check the regulatory update feed.
Monthly: Update compliance statuses as controls progress.
Quarterly: Re-run gap analyses to measure progress.
During incidents: Use the Incident Reporter immediately.

7 Framework & Deadline Reference

Quick-reference tables for all supported frameworks and incident reporting deadlines.

Supported Frameworks

🇮🇱 ISRAEL

- **Amendment 13**
  Privacy Protection Regulations · 15 controls
  Data protection, privacy rights, breach notification, and organizational security measures.

- **INCD Methodology**
  National Cyber Directorate · 12 controls
  Critical infrastructure protection, national cyber defense, incident response standards.

- **Draft Cyber Bill**
  January 2026 Draft · 10 controls
  Comprehensive cyber regulation including board accountability and mandatory risk management.

🇺🇸 UNITED STATES

- **NIST CSF 2.0**
  February 2024 · 16 controls
  Risk management framework covering Govern, Identify, Protect, Detect, Respond, Recover.

- **SOC 2**
  Trust Service Criteria · 12 controls
  Service organization controls for security, availability, processing integrity, and privacy.

- **CMMC Level 2**
  DoD Requirement · 11 controls
  Defense contractor cybersecurity maturity, CUI protection, and supply chain security.

Incident Reporting Deadlines

REGULATOR	TRIGGER	DEADLINE	WHERE
INCD (mandatory)	Critical infrastructure incident	6 hours	Israel
INCD (voluntary)	Significant cyber event	24 hours	Israel
Israel PPA	Personal data breach	72 hours	Israel
CIRCIA	Covered cyber incident	72 hours	USA
California AG	CA resident personal data breach	72 hours	USA
NY AG / DFS	NY resident personal data breach	72 hours	USA
DIBCAC	CUI-related incident	72 hours	USA
SEC (8-K)	Material cybersecurity incident	96 hours	USA

IMPORTANT

All deadlines are calculated from the **discovery date** you provide. Regulatory clocks don't start when you finish investigating — they start when you become aware. Document discovery time precisely.

Security & Deployment

ASPECT	DETAIL
Architecture	Self-hosted Next.js application. Your compliance data never leaves your infrastructure.
Database	SQLite — single local file, easy to back up and audit.
Network	Fully offline after initial setup. No external API calls.
Authentication	MVP: single-tenant, deploy behind corporate VPN. Multi-tenant auth planned for SaaS release.

ComplianceBridge v1.0

Built for the Israel-USA regulatory corridor.

Stop doing compliance twice.