Continuous Compliance for Critical Infrastructure

The Context GRC™ Capabilities Guide

For CISOs and Compliance Leaders in Electric, Water, Oil & Gas, and the Defense Industrial Base

Version 1.2 | October 2026

GoEvolve Assurance

Contents

The Problem: Compliance That Only Looks Backward 3
Continuous, Not Periodic: The Drift Engine 3
How a change travels 4
Capability Pillars 5
Cyber-Physical Asset Graph 5
Frameworks & Crosswalks 5
Policies & Controls 6
Evidence Hub 6
Risk Management 6
Action Center 7
Audit Portal 7
Sovereign AI That Stays in Your Network 7
Air-Gapped and Federal-Aligned 9
Security & Data Protection 9
Sector Playbooks 10
Electric: NERC CIP 10
Water: AWIA 10
Oil & Gas 10
Defense Industrial Base: CMMC 10
Other sectors 10
Integration & Extensibility 11
Deployment, Licensing & Ownership 11
Differentiation Matrix 11
Roadmap 12
Appendix A: Compliance Alignment 12

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

The Problem: Compliance That Only Looks Backward

Critical infrastructure operators answer to many mandates at once: NERC CIP, AWIA, CMMC, NIST frameworks, and sector rules that keep changing. Most programs still run on a calendar. Evidence is gathered before an audit, risk registers are refreshed when someone remembers, and the asset list in the spreadsheet drifts away from the plant.

The cost shows up between audits. A policy is revised and the mapped controls go stale. A server is added to a protected network and no one scopes it. Evidence expires quietly. By the time the next assessment arrives, the program is reconstructing history instead of managing risk.

Three realities make this harder for critical infrastructure:

- **Operational technology and IT live in one compliance boundary.** Electronic and physical security perimeters, shared infrastructure, and cyber-physical systems need to be modeled, not just listed.
- **Many environments cannot reach the internet.** Cloud-only tools are not an option for isolated networks, and sending compliance data to a third party is a risk in itself.
- **Auditors want traceable proof.** Every control, every piece of evidence, and every decision needs an owner, a date, and a link back to its source.

Context GRC™ is a continuous compliance platform designed for exactly this setting. It runs inside your network, keeps your data under your control, and watches for change so your team acts when something drifts, not months later.

Continuous, Not Periodic: The Drift Engine

At the center of Context GRC is the **Drift Engine**. It watches for changes across your policies, frameworks, assets, evidence, and risks, and routes the consequences to the people who own them.

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™



WHAT IT DOES

Thirteen engines run in two families. Six **positive** engines build forward momentum: document approval acceleration, OLIR control mapping harmonization, evidence renewal guidance, morning briefings, policy blast-radius alerts, and the AI telemetry learning flywheel. Seven **negative** engines protect against decay: dynamic ERT requirement gap sweeps, asset coverage gaps, evidence expiry, risk rollup, framework version crosswalk delta analysis, orphan cleanup, and statutory retention purge.

WHY IT MATTERS

Each facility or environment keeps its own engine settings. Administrators can switch any engine on or off per context and run it on demand, and every run or skip is recorded for the audit trail.

Scheduled engines run on their own cadence: risk scores recalculate every five minutes from control health, a morning briefing arrives at 07:00 in each context's local time, and retention purge and orphan cleanup run daily.

How a change travels

A change in…	Triggers…	You see…
Policies & Controls	Mapped controls are flagged for review	Owner notification and a blast-radius view

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

A change in…	Triggers…	You see…
Evidence Hub	Expired evidence marks the control and raises exposure	Renewal task and recalculated risk
Asset Inventory	A new asset needs control scoping	Coverage gap surfaced from the inventory
Frameworks	A revised mandate or new deployment evaluates mappings	Gap task or suggested OLIR control mapping in the Action Center

The evidence-expiry check, the OLIR control mapping drift scan, and the framework version crosswalk drift scan can be run on demand at any time. The asset coverage check reads your inventory; it does not scan your network.

> **ON THE PLANT FLOOR**
>
> Per-context engine settings let a NERC CIP Medium Impact boundary run on a different cadence from the corporate IT boundary. Each keeps its own configuration and audit history.

Capability Pillars

Seven integrated modules share one data model, so a change in one is visible in the others. A universal Command Palette (`Cmd+K` / `Ctrl+K`) and declarative deep-link routing let operators jump directly to any framework, requirement, policy, control, risk, action plan, action item, asset, or evidence artifact with slide-out detail drawers.

Cyber-Physical Asset Graph

The asset inventory models what actually sits in your regulatory boundary. It supports 14 asset types, including facilities, electronic security perimeters, physical security perimeters, shared cyber infrastructure, and systems of systems. Assets nest in parent and child hierarchies, and 11 regulatory traits (such as ERC, ESP, PSP, EAP, TCA, and removable media) tag each asset for the standards that care about it.

Population lists that NERC CIP programs normally maintain by hand come from the data. Electronic access point and transient cyber asset populations derive from traits. A full ERT Level 1 population workbook (13 tabs) exports on demand. You can also compare an uploaded ERT template against the live inventory to see where they have drifted, and find gaps dynamically.

Bulk import accepts CSV and Excel files with saved column mappings, and any grid exports to CSV.

> **ON THE PLANT FLOOR**
>
> Model an ESP and its access points once. The same objects feed CIP-002 categorization, CIP-005 perimeter evidence, and your ERT workbooks.

Frameworks & Crosswalks

Context GRC ships with a catalog of 40 frameworks and standards, including all 15 NERC CIP standards (CIP-002 through CIP-015), the AWIA Section 2013 requirements, FedRAMP Low, Moderate and High baselines,

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

NIST SP 800-53 Rev. 5 and 800-171 Rev. 2, NIST CSF 2.0, CMMC Levels 1 and 2, ISO 27001, 27002 and 27701, SOC 2, HIPAA, PCI DSS 4.0, CIS Controls v8, GDPR, and CCPA.

Seven prepackaged NIST-based crosswalks hold 69 mappings, linking 800-53 to AWIA, ISO 27001, SOC 2, FedRAMP Moderate and High, and NERC CIP, and CSF 2.0 to AWIA. Map once and see coverage across frameworks. With 1-click evidence inheritance, verified proof attached to a baseline control links directly to equivalent target controls through database pointers without duplicating stored files. When new frameworks are deployed or controls are updated, the OLIR Control Mapping Drift Engine scans for unmapped equivalents via authoritative crosswalks and vector similarity, staging mapping proposals while permanently respecting prior human rejections.

The prepackaged catalogs are curated working sets. They are not a substitute for the authoritative text of each standard.

Policies & Controls

Bring policies in from five channels: file or ZIP upload, document-ID URL, SharePoint, Confluence, and Git repositories. Background workers extract text and propose controls using AI. Nothing is added to your control library until a person approves it.

A unified 4-touchpoint Human-in-the-Loop (HITL) triage system surfaces pending items in the top app bar, Dashboard domain review pills, in-module slide-out triage drawers, and a consolidated Review Queue with source-module filters. Reviewers approve or reject proposed controls, requirements, and crosswalk mappings one by one or in bulk, and can assign owners in bulk. When a policy is revised, the Drift Engine alerts the owners of every mapped control.

Evidence Hub

Evidence lives in S3-compatible object storage with encryption at rest. Artifacts can be bound directly to regulatory requirements as well as internal controls, tracking provenance across direct uploads, control synchronization, AI extractions, and continuous compliance retention. When a control is unmapped or retired, linked evidence is automatically retained on the underlying requirement (`CONTINUITY_RETAINED`) so audit history is never orphaned. Each item carries an expiry date, so renewal becomes a planned task instead of an audit surprise. Deleted evidence moves to a recycle bin and can be restored, so nothing disappears without a trail.

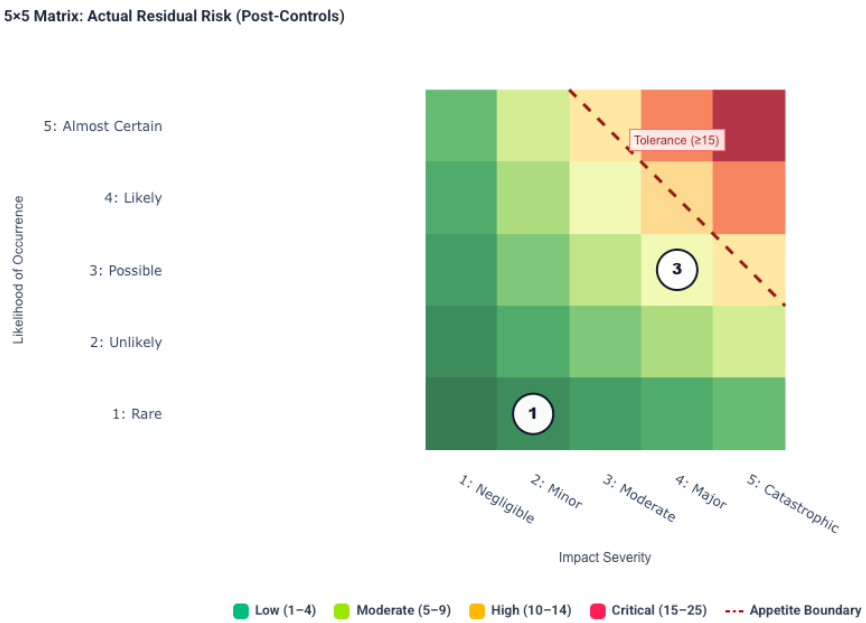
Every module action lands in a hash-chained audit ledger, which makes after-the-fact edits detectable.

> **ON THE PLANT FLOOR**
>
> Expiry tracking helps CIP-007 patching records and CIP-010 baseline evidence stay current, because the engine raises a renewal task before the evidence goes stale.

Risk Management

Quantify risk in financial terms with single loss expectancy, annual rate of occurrence, and annualized loss expectancy. A 5×5 heatmap compares inherent and residual risk against your appetite boundary.

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™



Guided EBIOS RM assessments walk teams through five workshops. Risk acceptance records the approver, rationale, and date. AI-suggested mitigations arrive as proposals that a person applies or dismisses.

Action Center

Remediation work lives in Kanban, list, and matrix views. Root-cause guidance supports 8D and 5-Why methods, so corrective actions address causes, not symptoms. Work raised by the Drift Engine and by AI review lands here, so owners see one queue.

Audit Portal

Auditors get a dedicated workspace with five views: engagement builder, matrixed mandates, overlay catalog, evidence vault, and audit trail. Access is limited to auditor and administrator roles. Evidence harvesting runs in parallel across the assets you select.

The NERC ERT Level 2 overlay (version 10.1) is prepackaged with 170 requests, 71 sample sets, and 21 standards. Import and deploy overlays, and search the audit log by severity and source.

Sovereign AI That Stays in Your Network

AI features run on local models by default. The platform profiles the host hardware and picks the model, thread count, and context window that fit, from a workstation to a GPU server.

For regulatory reasoning, model-aware thinking depth (`off`, `low`, `full`) across DoD-favorable open-weight model families (**IBM Granite**, **Microsoft Phi**, and **Mistral-Nemo**) balances speed with analytical rigor. Routine inventory lookups run with zero reasoning overhead for sub-second responses, while complex multi-clause regulatory deductions dynamically allocate internal chain-of-thought scratchpads to analyze intricate cross-

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

standard requirements. Internal reasoning traces are automatically stripped before presenting clean, audit-ready outputs.

The **Catalyst AI Resident Consultant** operates in both a contextual edge drawer and a full-screen workspace (`/catalyst`) with persistent session history, shareable deep links, and a dual-pane **Policy Canvas** for live side-by-side markdown drafting and export. Five specialty personas (Policy, Audit, Drift, Remediation, and Crosswalk) are grounded in live context-scoped records and tailored by per-boundary **AI Context Profiles** that describe each facility's operational architecture.

Administrators who choose to can point the platform at an OpenAI-compatible inference endpoint that they host. That decision belongs to your organization, and it is a deliberate setting.

CONTEXT GUARDIAN: INDEPENDENT AI-ON-AI VERIFICATION & BUSINESS RULE SUBSTITUTION

Single-model compliance assistants suffer from a well-known risk: the model that generates an analysis grades its own confidence. Context GRC eliminates this with **Context Guardian**, powered by an independent local judge model—**IBM Granite Guardian (`granite4.1-guardian:8b`)**:

- **Groundedness Verification:** Checks drafted controls, root cause analyses, and crosswalk deltas against authentic source documents before rendering or applying them.
- **Business Rule Enforcement & Compliant Substitution:** Evaluates AI recommendations against mandatory organizational policies. When a non-compliant option is detected (such as external cloud MFA), Context Guardian automatically substitutes the pre-approved compliant alternative (such as On-Premises RADIUS/TACACS+ MFA) while de-duplicating against sibling options.
- **Two-Key Evidence Gate:** Evidence is never auto-accepted based on a single model's score. Auto-acceptance requires both primary pass confidence and a clean Granite Guardian groundedness verdict; otherwise, it is staged for human review.
- **Boundary & Agentic Protection:** Screens incoming prompts for jailbreaks, blocks destructive SQL or unauthorized privilege escalations, and verifies outbound payloads before transmission if external endpoints are used.
- **Measurable Protection & Value Scorecard:** Administrators monitor tangible ROI through an executive 4-KPI banner tracking total outputs screened, disallowed controls auto-substituted, ungrounded hallucinations intercepted, and unsafe queries blocked.
- **Universal Auto-Adoption:** Every present and future AI capability built on Context GRC automatically inherits Context Guardian protection through the centralized AI gateway.

ACCOUNTABLE BY DESIGN

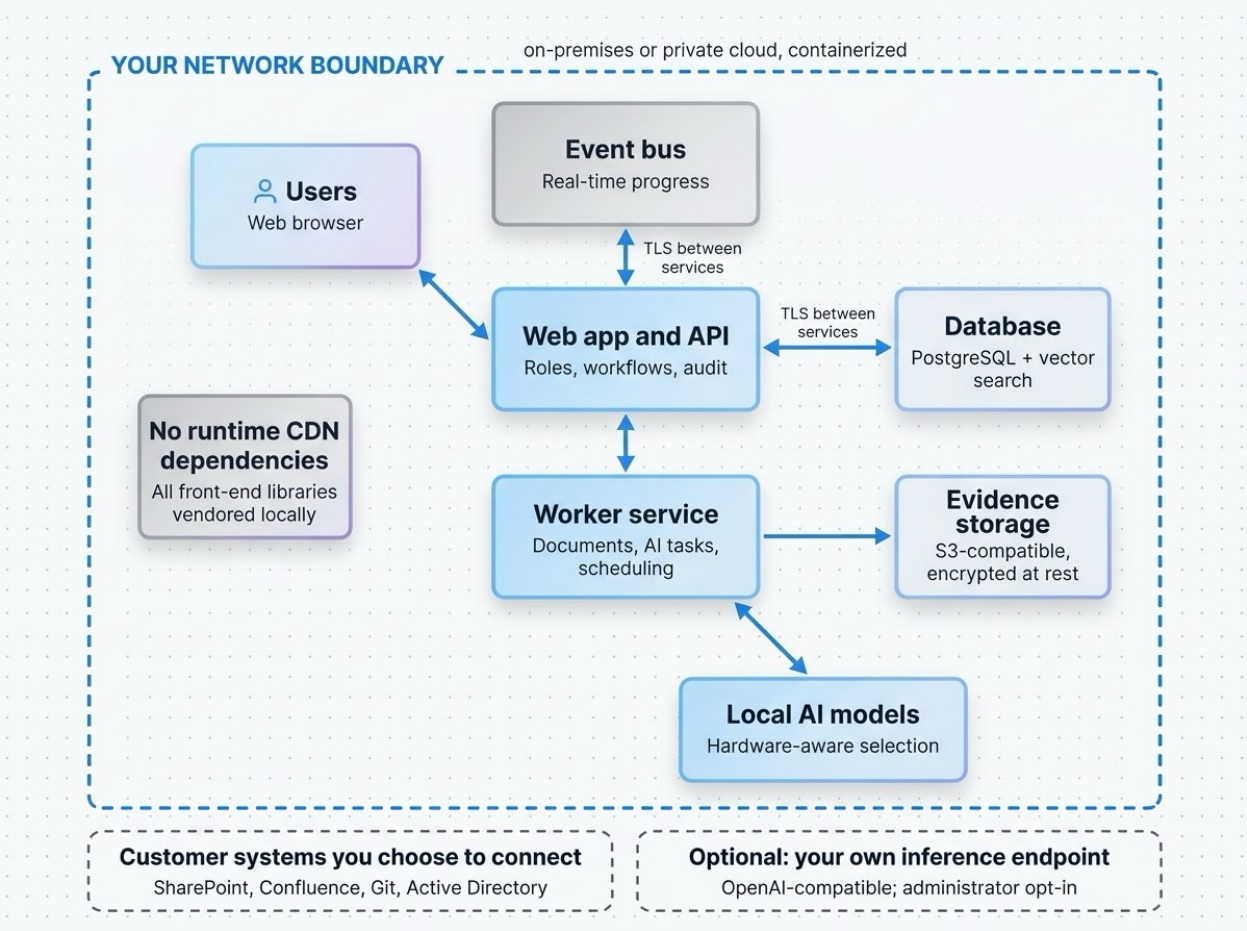
Every assistant query records who asked, in which context, which model answered, how long it took, the response, and the source passages it cited. Human corrections feed an AI telemetry loop. Long-running AI jobs report live progress over WebSockets, with no polling.

AI proposes. People decide. Extracted controls and suggested mitigations wait in a review queue for explicit human approval before they change your data.

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

Air-Gapped and Federal-Aligned

Context GRC deploys as a containerized stack on premises or in a private cloud. Every front-end library is vendored locally with documented licenses and SHA-256 manifests, so there are no runtime calls to public content networks. That makes it suitable for networks with no internet path.



For supply chain scrutiny, the dependency inventory is hash-verified and exactly pinned through a uv lockfile covering 177 packages and about 3,000 SHA-256 hashes. Continuous integration gates builds with static analysis, secret scanning, a strict vulnerability audit, a copyleft license gate, and filesystem scanning.

> **ON THE PLANT FLOOR**
>
> Run it entirely inside a management network adjacent to your ESP. The front end makes no calls to public content networks, and AI runs locally by default.

Security & Data Protection

- **Authentication.** Passwords are hashed with PBKDF2-HMAC-SHA256 at 600,000 iterations with NIST SP 800-63B passphrase policy enforcement. Active Directory (LDAP/LDAPS) authentication supports multi-select security

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

group filtering, Just-In-Time (JIT) provisioning, and 15-minute directory sync. TOTP multi-factor authentication is built in, with optional 30-day trusted devices.

- **Secrets.** Integration credentials are encrypted at rest with Fernet and can be rotated with a supplied script. Service secrets are injected through Docker secrets.
- **Transport and storage.** Services communicate over TLS. Evidence storage is encrypted at rest.
- **Role-based access and worker isolation.** Roles are granted per context, and views are scoped to the active context. Background AI workers execute under least-privilege PostgreSQL Row-Level Security (`grc_worker`), verify Ed25519-signed task envelopes (`SignedTaskEnvelope`), screen prompts through a pre-persistence DLP engine, and fence untrusted document extracts against indirect prompt injection.
- **Tamper-evident audit.** A hash-chained ledger records actor, context, timestamp, and outcome for module actions.

Sector Playbooks

Electric: NERC CIP

Start with all 15 CIP standards in the catalog. Model BES Cyber Systems, ESPs, and PSPs in the asset graph, generate ERT Level 1 workbooks, and bring the Level 2 overlay into audit preparation. The Drift Engine keeps the evidence and asset records current between audits.

Water: AWIA

The AWIA Section 2013 catalog and two prepackaged crosswalks (from 800-53 and from CSF 2.0) give risk and resilience assessment teams a starting structure. The risk module's financial view supports the cost-of-impact discussions that boards expect.

Oil & Gas

Pair NIST 800-53 and CSF 2.0 with the cyber-physical asset graph to scope pipeline, terminal, and facility assets. Sector-specific catalog content can be added through your own policies and controls.

Defense Industrial Base: CMMC

CMMC Levels 1 and 2 and NIST 800-171 Rev. 2 are in the catalog. Local AI and air-gapped deployment keep controlled information inside your boundary.

Other sectors

Sector	Where to start
Healthcare	HIPAA catalog plus ISO 27001 and SOC 2
Financial services	PCI DSS 4.0, SOC 2, and NIST CSF 2.0
Federal contractors	FedRAMP baselines, 800-53, and 800-171
Commercial enterprise	ISO 27001, SOC 2, GDPR, and CCPA

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

Integration & Extensibility

All connectors are administered in one place, under System Administration. Policy content flows in from SharePoint (on-premises Subscription Edition and Online), Confluence spaces, and GitHub or GitLab repositories. An Active Directory connector (LDAP or LDAPS) supports both platform authentication (with security group filtering and 15-minute sync) and automated directory-state evidence collection. Domain modules reuse those central connection settings, so credentials are never scattered across screens.

Deployment, Licensing & Ownership

You deploy Context GRC where you choose: on premises or in a private cloud, as containers. Your data stays in your environment.

- **Offline license verification.** Licenses are Ed25519-signed tokens verified locally. There is no phone-home, so air-gapped sites work the same as connected ones.
- **Tiers by scope.** Limits apply to the number of contexts and internal users, so a single facility and a multi-site utility both have a fitting tier.
- **Free Auditor.** Auditor accounts never consume a seat, so your assessors and regulators never add cost.
- **Graceful expiry.** After a 14-day grace period, the platform moves to a read-only archive mode. It never locks you out of your own records.

Differentiation Matrix

Most organizations compare Context GRC with five common approaches. The table describes what these approaches typically offer.

Need	Legacy enterprise GRC suite	Workflow platform with a GRC module	Cloud compliance automation SaaS	Federal authorization toolchain	Spreadsheets & shared drives	Context GRC
Runs fully on premises or air-gapped	Often	Sometimes	Rarely	Often	Yes	Yes
Local AI with source citations	Rarely	Rarely	Rarely	Rarely	No	Yes
Cyber-physical asset modeling (ESP, PSP, SCI)	Rarely	Rarely	Rarely	Sometimes	Manual	Yes
NERC CIP content prepackaged	Sometimes	Rarely	Rarely	Rarely	Manual	Yes

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

Need	Legacy enterprise GRC suite	Workflow platform with a GRC module	Cloud compliance automation SaaS	Federal authorization toolchain	Spreadsheets & shared drives	Context GRC
Continuous drift detection	Rarely	Sometimes	Often	Sometimes	No	Yes
Offline license verification	Rarely	Rarely	No	Sometimes	Not applicable	Yes
Auditors at no seat cost	Rarely	Rarely	Rarely	Rarely	Yes	Yes

This table reflects general market patterns and each organization's own evaluation will vary.

Roadmap

> ***Planned items.*** *The following are direction, not commitments for a specific date.*

- **Signed offline installers and update bundles.** Verifiable packages for sites that move software across an air gap by hand.
- **Additional evidence connectors.** Automated pulls from cloud infrastructure and device management platforms.
- **Expanded sector content.** More catalog content for oil and gas and other critical infrastructure sectors.

Appendix A: Compliance Alignment

Context GRC is designed to support, and helps you prepare for, the programs below. It is aligned to the control families these programs use, and it is not itself certified, authorized, or accredited under any of them.

Program	How Context GRC helps
NERC CIP	Asset population, ESP and PSP modeling, ERT workbook exports, and evidence tracking
AWIA Section 2013	Prepackaged requirements and crosswalks for risk and resilience assessments
CMMC and NIST 800-171	Catalogs, evidence tracking, and gap tasks
FedRAMP baselines	Aligned to the baseline control sets to help customers who seek authorization
NIST CSF and 800-53	Catalogs, crosswalks, and risk quantification

Context GRC supports customers' compliance programs; it does not itself confer certification or authorization. Prepackaged framework catalogs are curated working sets and do not replace authoritative standards text.

© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™

Ready to see it in your environment?

Request a briefing: **goevolve.com** | **info@goevolve.com**



© 2026 GoEvolve LLC, DBA GoEvolve Assurance. Context GRC™