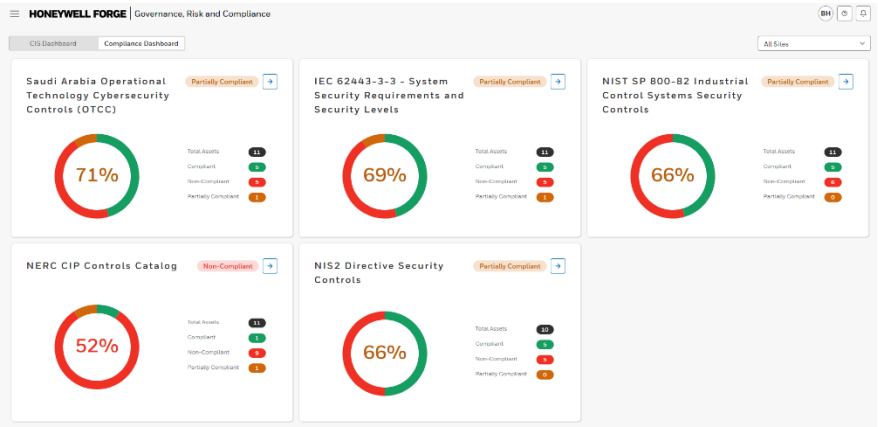
HONEYWELL CYBER GOVERNANCE, RISK, AND COMPLIANCE (GRC)

Introducing Honeywell Cyber Governance, Risk, and Compliance (GRC), a purpose-built compliance automation platform designed specifically for industrial operations and critical infrastructure.

Honeywell Cyber GRC is a SaaS-based compliance automation platform purpose-built for OT and ICS environments. It helps streamline regulatory adherence by centralizing framework mapping, evidence collection, and compliance scoring across industrial sites. Designed for regulated sectors, the platform incorporates preloaded OT-specific frameworks, CIS Benchmarks, and AI/ML-driven policy parsing to transform manual, document-heavy processes into automated, repeatable workflows.

By replacing fragmented, spreadsheet-driven practices, Cyber GRC can significantly reduce manual compliance burden and accelerate audit readiness. Unified dashboards provide clear visibility across assets, controls, and regulatory obligations, helping organizations to monitor posture continuously and present executive-ready insights. The result is a more efficient, consistent, and scalable approach to managing compliance across multi-site industrial operations.



WHY CYBER GRC

AI-Powered Mapping
Mapping unstructured policies into structured requirements.

Built-in Library
Major OT/ICS regulatory frameworks. Designed to continuously expand as regulations evolve.

CIS Benchmarks
The compliance engine includes twenty-five (25) CIS benchmarks. Designed to continuously expand.

Centralized Dashboard
Compliance dashboards with percentage scoring across frameworks, controls, and assets.

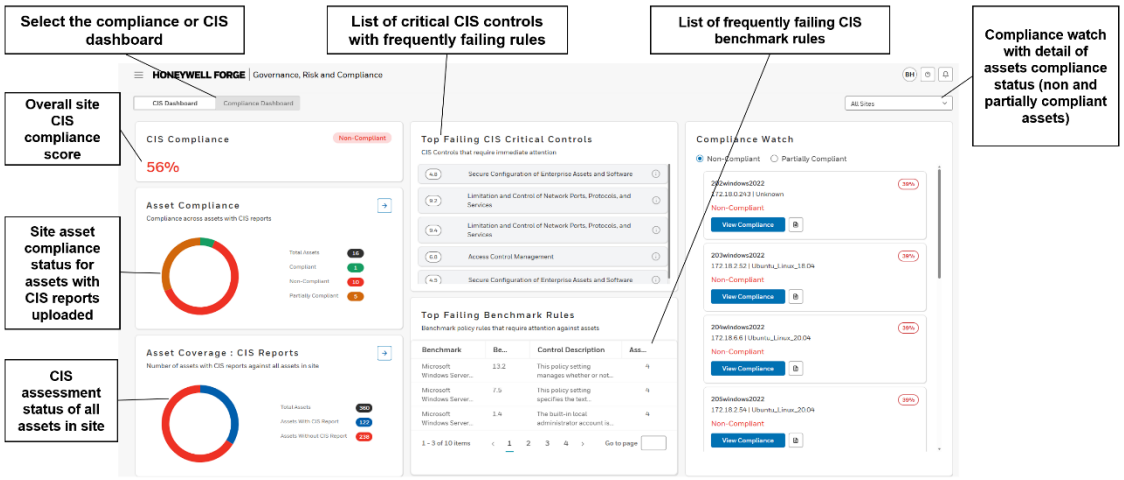
Remediation Tracking
Workflow-driven remediation tracking and executive-ready reporting.

Designed for OT
OT Compliance-focused for critical infrastructure.

CYBER GRC FEATURES AND BENEFITS

- **Automated OT/ICS Compliance at Scale:** Cyber GRC replaces fragmented, spreadsheet-driven compliance workflows with automated, continuous monitoring across multiple OT/ICS frameworks. With built in support for 5 OT regulatory frameworks and automated percentage-based compliance scoring, it helps organizations to dramatically reduce manual reporting, audit preparation time, and human error.
- **AI/ML-Driven Policy Parsing & Evidence Collection:** A differentiating capability, Cyber GRC uses AI/ML to convert unstructured policy documents, often tens of thousands of requirements, into structured, actionable compliance data. This enables automated mapping of 25 CIS Benchmarks to OT frameworks and reduces dependence on manual interpretation. Combined with automated evidence ingestion and audit-ready traceability, organizations can achieve faster, more accurate assessments with far less manual work.
- **Unified Dashboard for Enterprise-Wide Visibility:** Cyber GRC provides a single, centralized dashboard that consolidates compliance posture across sites, assets, benchmarks, and frameworks. This “single pane of glass” gives compliance managers, CISOs, and executives immediate insight into site readiness, control gaps, and remediation progress. It solves a major pain point, lack of board-ready visibility into OT cyber posture by delivering consistent, standardized reporting across the enterprise.
- **Purpose-Built for OT/ICS Environments:** Unlike IT-centric GRC platforms that require heavy customization, Cyber GRC is designed specifically for OT operations in energy, oil & gas, manufacturing, utilities, chemicals, maritime, pharma, and other regulated industrial sectors. It incorporates OT-specific frameworks (e.g., NIST 800-82, NIS2, IEC 62443-3-3, NERC CIP, OTCC) and aligns compliance scoring with operational assets. This OT-first approach ensures more accurate mapping, deeper contextual relevance, and seamless integration with Honeywell’s broader OT cybersecurity ecosystem.

CYBER GRC DASHBOARD



CYBER GRC FEATURES & BENEFITS

Customer Pain Point	Cyber GRC Feature	Customer Benefit
Fragmented, manual compliance processes across multiple sites.	**Automated compliance engine** with built-in **5 OT/ICS frameworks**, CIS benchmark ingestion, and **centralized evidence repository**; **workflow-driven remediation** across sites.	Eliminates spreadsheets and duplicated effort, standardizes processes across all sites, and can shorten audit prep through automation and centralized control.
High cost of manual reporting (3–4 FTE, ~$250K per site/year).	**AI/ML-driven policy parsing + automated evidence collection** and percentage-based compliance scoring reduce human touchpoints.	Cuts manual workload and reporting cycles, enabling reductions in compliance costs and freeing teams to focus on higher-value tasks.
Increasing regulatory complexity across 300+ frameworks.	**OT-first framework library** (e.g., NIST 800-82, NIS2, IEC 62443-3-3, NERC CIP) with **AI-accelerated mapping of 25 CIS Benchmarks** into OT controls for continuous alignment.	Simplifies cross-walks and keeps pace with evolving obligations, helping reduce interpretation errors and improving consistent compliance across regions and standards.

Lack of board-level visibility into cyber posture.	**Unified, executive-ready dashboards & reports** showing compliance by framework, control, and asset, with remediation status and trends.	Delivers a clear, "single pane of glass" for leadership to track readiness, quantify gaps, prioritize investments, and demonstrate governance.

CYBER GRC SPECIFICATIONS

Category	Specification / Detail
Platform Type	SaaS-based OT/ICS compliance automation platform.
Primary Use Cases	Regulatory adherence, evidence collection, framework mapping, continuous compliance tracking, and audit readiness for industrial/critical infrastructure sectors.
Core Data Inputs	CIS Benchmark outputs (automated ingestion) and unstructured policy documents converted to structured requirements via AI/ML.
Evidence Handling	Centralized evidence repository with automated evidence collection and traceable audit trails.
Compliance Scoring	Percentage-based compliance scoring at framework, control, and asset levels; site-level roll-ups.
Dashboards & Reporting	Unified, executive-ready dashboards; multi-site reporting; remediation status and trends.
AI/ML Capabilities	AI/ML-driven parsing of unstructured policies into structured requirements; automated mapping of CIS Benchmarks to OT frameworks.
Asset Context	Asset inventory/attributes included in assessments; control checklist validation.
Access & Scale	Role-based access and multi-site reporting for enterprise-wide oversight.
Configuration (Setup)	Preloaded OT framework library, low-complexity experience compared to risk-heavy legacy platforms.
Configuration (Scoring & Mapping)	Built-in mappings between CIS Benchmarks and OT frameworks; configurable control validations
Commercial Model (High-Level)	Per-seat / per-audit-oriented packaging.

CYBER GRC SUPPORTED COMPLIANCE FRAMEWORKS & BENCHMARKS

Item	Details
OT/ICS Framework Library (Total)	5 preloaded OT/ICS frameworks purpose-built for industrial environments. Examples include NIST 800-82, IEC 62443-3-3, NIS2, and NERC CIP.
Benchmarks Integrated	25 CIS Benchmarks integrated into the compliance engine for automated compliance calculations and evidence ingestion.
Mapping Automation	AI-accelerated mapping of CIS Benchmarks to OT frameworks to reduce manual interpretation, increase accuracy, and maintain continuous alignment.

For more information
www.honeywell.com/cybersecurity

Honeywell
855 Mint St Charlotte
NC, 28202-1517
USA
www.honeywell.com

THE FUTURE IS WHAT WE MAKE IT

Honeywell