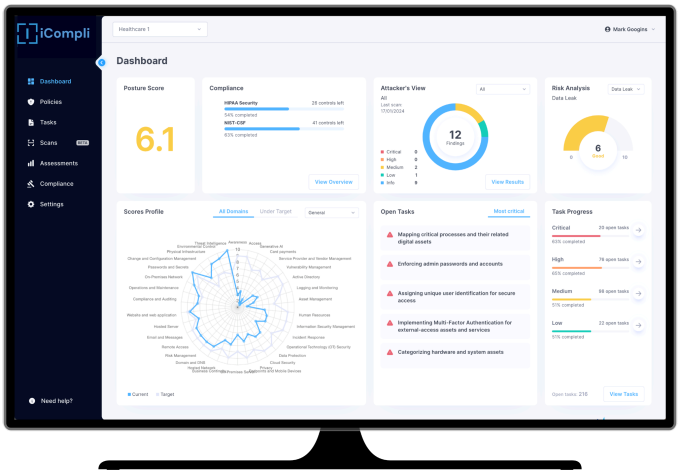
The Intelligent Security and Compliance Platform

2026

iCompli is an intelligent platform designed to operationalize cybersecurity and compliance leadership. Managing both **security risk** and **regulatory compliance** has become increasingly complex. Keeping up with frameworks, threats, audits, and remediation efforts often stretches internal teams beyond capacity. **iCompli** addresses this challenge head-on.



Automated Security and Compliance

iCompli brings together the two foundational elements of vCISO services: security and compliance, delivered in a **single, unified platform.** The platform enables: continuous security assessments, gap identification, compliance readiness tracking, policy generation, task orchestration, and executive-level reporting. **Everything is designed to be actionable, prioritized, and aligned with real business risk.**

iSHIFT

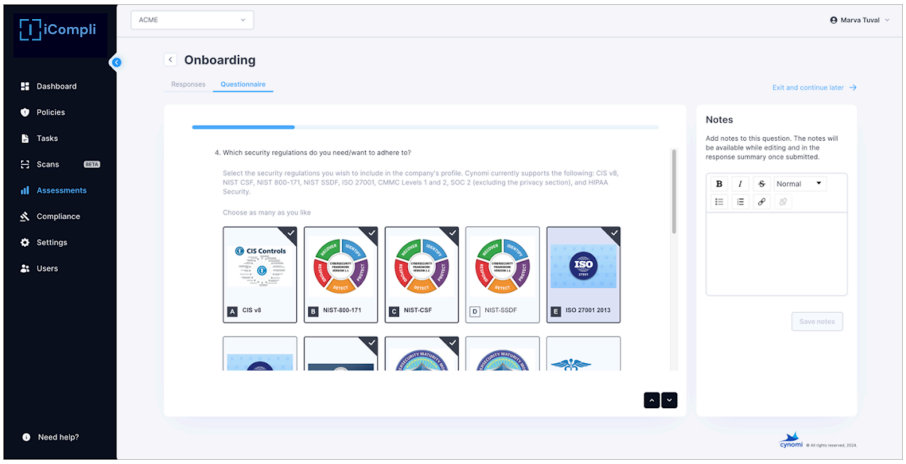
iCompli Capabilities

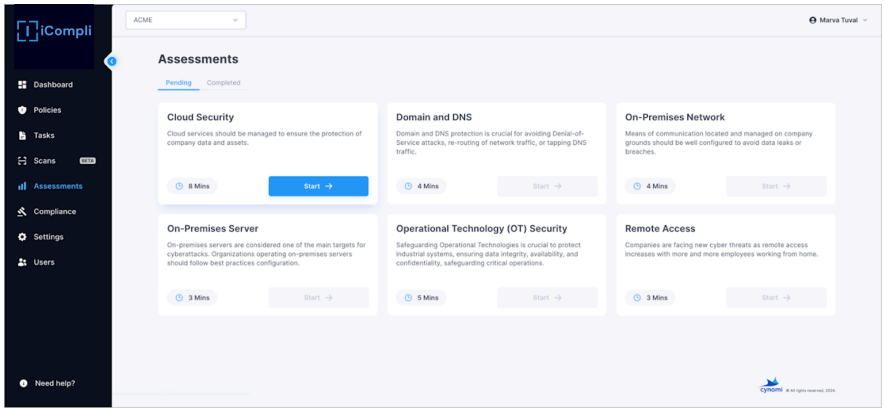
1. Client Onboarding and Environment Discovery
2. Internal and External Asset Scanning
3. Continuous Security Assessment
4. Framework-Based Compliance Management
5. AI Risk Management
6. Client-Specific Security Policies
7. Prioritized, Actionable Remediation Tasks
8. Risk Management and Third-Party Risk Oversight
9. Planning and Remediation Roadmap
10. Client-Ready Executive Reporting
11. Continuous Improvement by Design

Client Onboarding and Environment Discovery

Every engagement begins with structured onboarding to understand our client's **organization, industry, and technology landscape.** Together, we complete an initial high-level questionnaire covering infrastructure, users, applications, and operational context. Based on these responses, iCompli automatically generates targeted follow-up questionnaires focused on security posture and risk exposure.

Using this information, the platform builds a **tailored remediation strategy** and produces **customized security policies** aligned to our client's environment. As the organization evolves, questionnaires can be updated at any time, triggering **automatic policy and task adjustments to reflect the new reality.**





iSHIFT

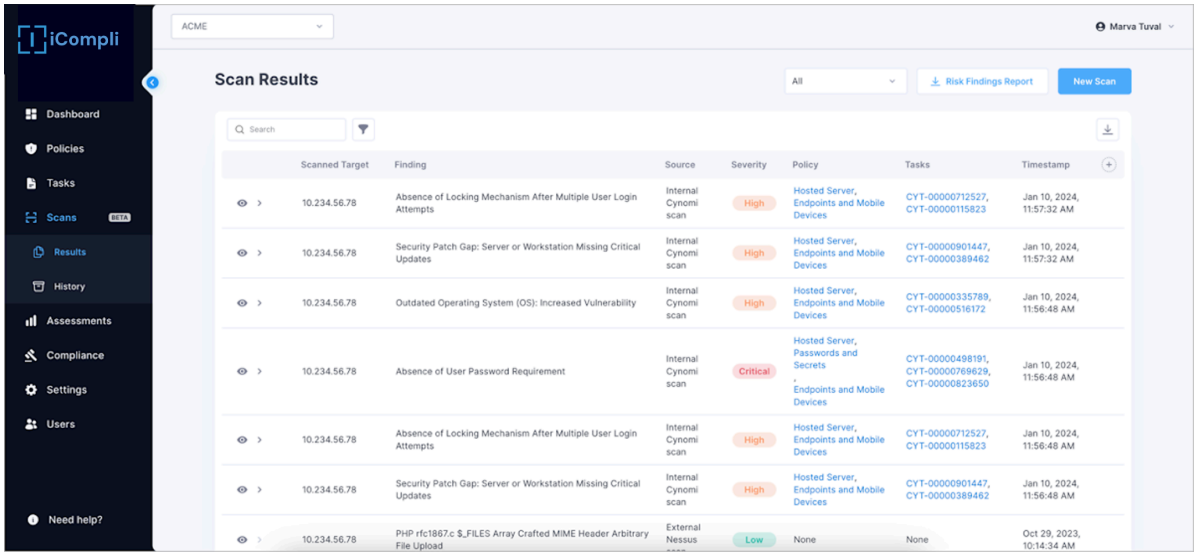
Internal and External Asset Scanning

To enrich questionnaire data and provide objective validation, iCompli incorporates **automated security scanning**.

External Scanning

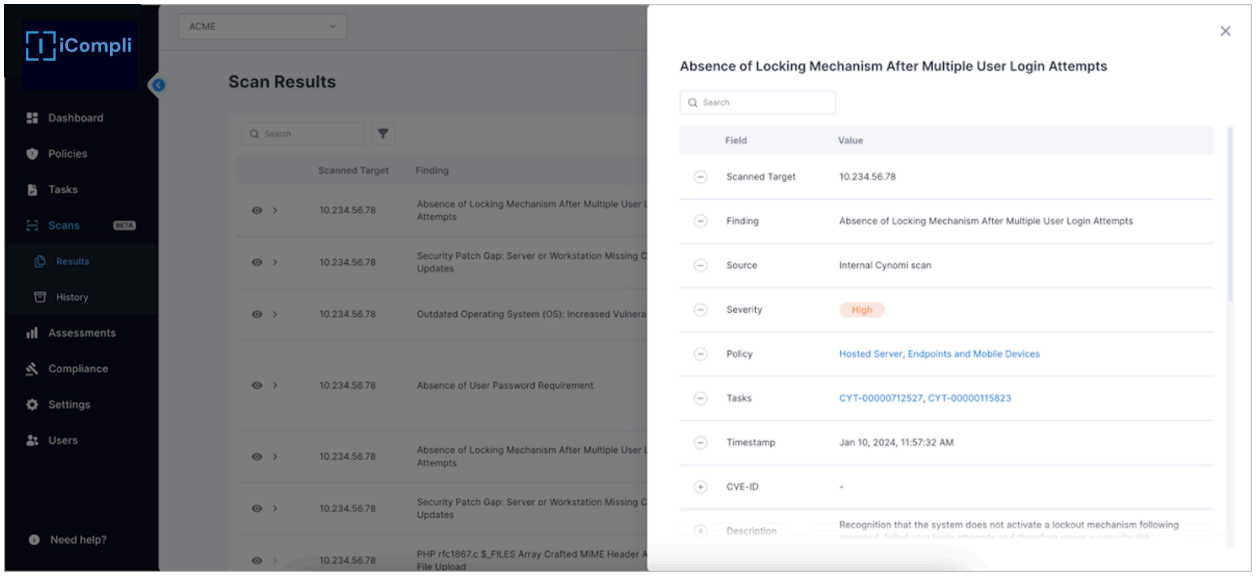
iCompli evaluates externally facing assets such as IP addresses and URLs to identify vulnerabilities and configuration weaknesses. This includes:

- **Open and risky ports**
- **Protocol and encryption validation**
- **Email security configuration checks**
- **Web application technology and patch levels**



Each finding includes **detailed context and remediation guidance**. Discovered issues are automatically converted into prioritized remediation tasks based on severity.

Scan results are available within minutes.



Internal Scanning

Internal scans assess **security hygiene across internal environments**, including assets such as Active Directory and endpoints. These scans identify misconfigurations, weak controls, and internal exposure risks.

Third-Party Scan Integration

iCompli also supports ingestion of results from tools such as Nessus, Qualys, and Microsoft Secure Score via CSV import.

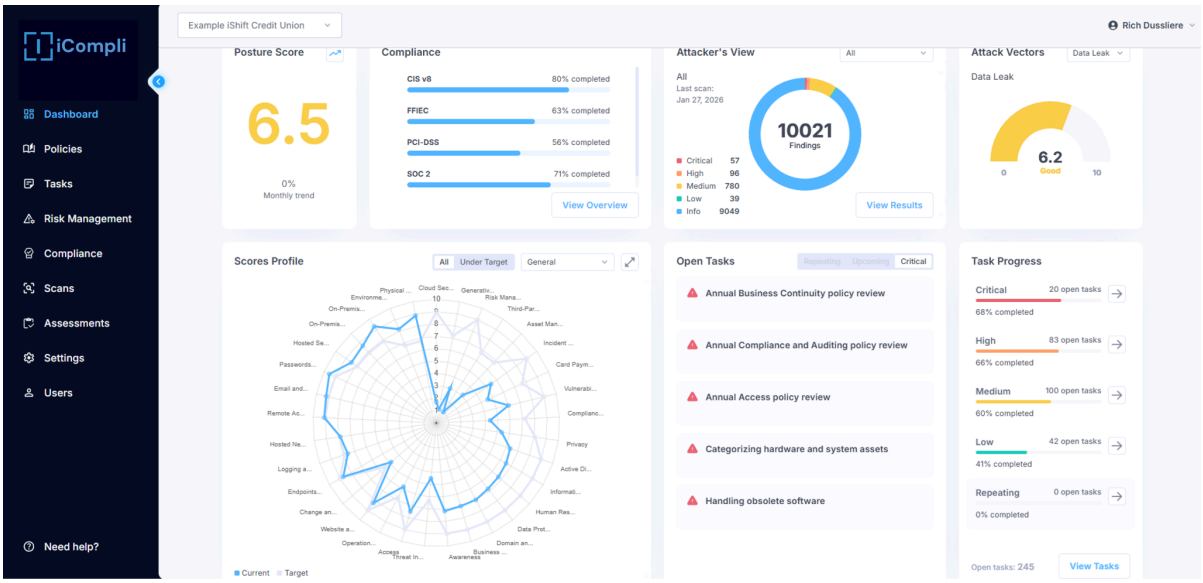
All scan findings are consolidated into a **single view and mapped directly to relevant policies, controls, and remediation tasks**.

Continuous Security Assessment

iCompli continuously evaluates each organization's cyber profile against applicable security standards, regulatory requirements, and industry-specific threat intelligence.

Scan results, questionnaire responses, and environmental context are correlated to **dynamically select the most relevant security domains and control requirements**. Each requirement is assigned a criticality rating reflecting its impact on the organization's risk profile.

Threat-based risk indicators, such as ransomware exposure or data leakage likelihood, are calculated based on business sensitivity and control maturity.



The result is a centralized, real-time view of security posture that tracks improvement over time.

Security Dashboard Highlights

The platform dashboard provides:

- **Overall security posture score**
- **Vulnerability and exposure gap analysis**
- **Risk scoring by threat category**
- **A prioritized, actionable remediation plan**
- **Visibility into compliance alignment across frameworks**

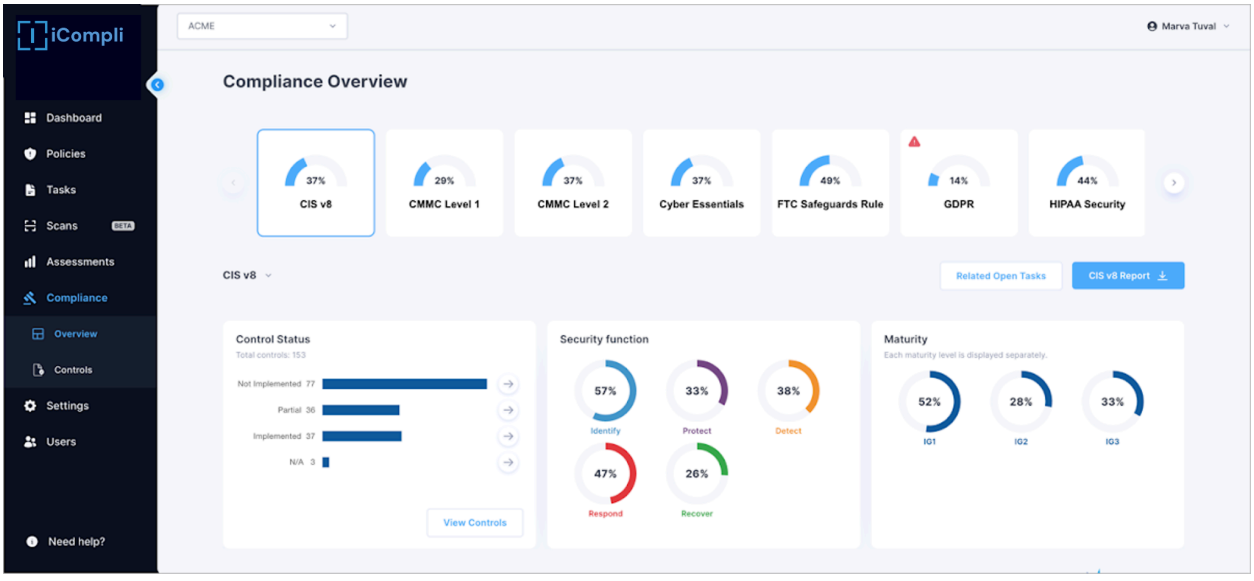
Framework-Based Compliance Management

iCompli continuously measures readiness across a broad and expanding set of **regulatory and security frameworks**, including:

- **CIS v8**
- **ISO 27001**
- **NIST CSF 1.1 and 2.0**
- **NIST 171 and SSDF**
- **SOC 2**
- **CMMC Levels 1 and 2**
- **GDPR, CCPA, NIS2**
- **PCI-DSS**
- **HIPAA Security Rule**
- **Cyber Essentials**
- **FTC Safeguards Rule**
- **SEC cybersecurity requirements**
- **ICS cybersecurity standards**
- **FFIEC guidance**
- **NIST AI RMF 1.0**

The compliance module allows users to **explore each framework in detail**, understand individual controls, and see how remediation tasks map across multiple standards simultaneously.

Compliance status is updated continuously, providing **real-time awareness** of readiness levels.



iSHIFT

Compliance Reporting

iCompli can generate dedicated compliance reports that include:

- **Overall compliance posture**
- **Control inventories**
- **Maturity levels**
- **Control implementation status**
- **Framework mappings**
- **Direct links to remediation tasks**

This enables **rapid gap identification** and fast creation of **framework-specific remediation plans** with minimal effort.

iSHIFT

AI Risk Management

The **NIST AI Risk Management Framework (AI RMF) 1.0** is a framework that provides a flexible and structured approach **to assess and govern the safety, reliability, and trustworthiness of AI technologies**.

The AI RMF is built around a set of Core Functions that guide organizations in identifying, measuring, and minimizing AI risks:

- **GOVERN: Embedding Risk Culture**

  Creates a culture of risk management, accountability, and oversight. Key subcategories include: policies for AI risk management, internal accountability structures, documentation, workforce training, stakeholder engagement, and third-party AI risk management.

- **MAP: Contextualizing AI Use Cases**

  Focuses on understanding context, including risks, impacts, and potential positive/negative outcomes. Key subcategories include: establishing context, identifying AI system components, categorizing systems, identifying risks, and documenting risk tolerance.

- **MEASURE: Quantifying Risk**

  Involves tracking and analyzing AI risks using both quantitative and qualitative methods. Key subcategories include: evaluating, testing, and monitoring AI systems for performance, safety, and fairness (bias), including human-AI interaction testing.

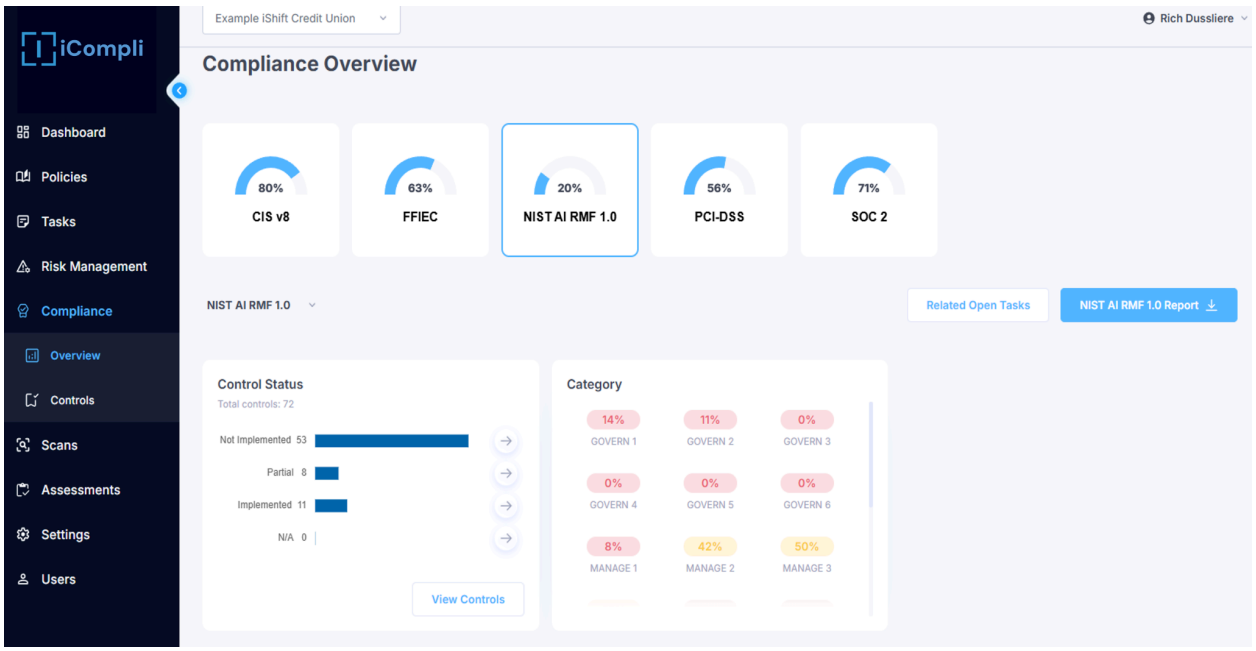
- **MANAGE: Operationalizing Risk Response:**

  Involves implementing, executing, and monitoring risk mitigation strategies. Key subcategories include: prioritizing risks, implementing mitigation strategies (including tracking residual risks), and managing risks in pre- and post-deployment.

NIST AI RMF helps organizations **manage the unique risks associated with AI systems**, including issues such as bias, security vulnerabilities, lack of transparency, and system drift.

Organizations implementing AI RMF typically focus on:

- **AI System Inventory:** Creating a comprehensive list of all AI systems.
- **Risk Assessment and Prioritization:** Categorizing AI systems by risk level.
- **Bias Mitigation:** Actively identifying and addressing harmful bias.
- **Continuous Monitoring:** Tracking system performance post-deployment.
- **Documentation:** Maintaining records of the risk management process.



AI RMF complements frameworks like **NIST CSF and ISO 27001** by focusing specifically on AI-related risk dimensions that traditional security frameworks don't fully address.

Client-Specific Security Policies

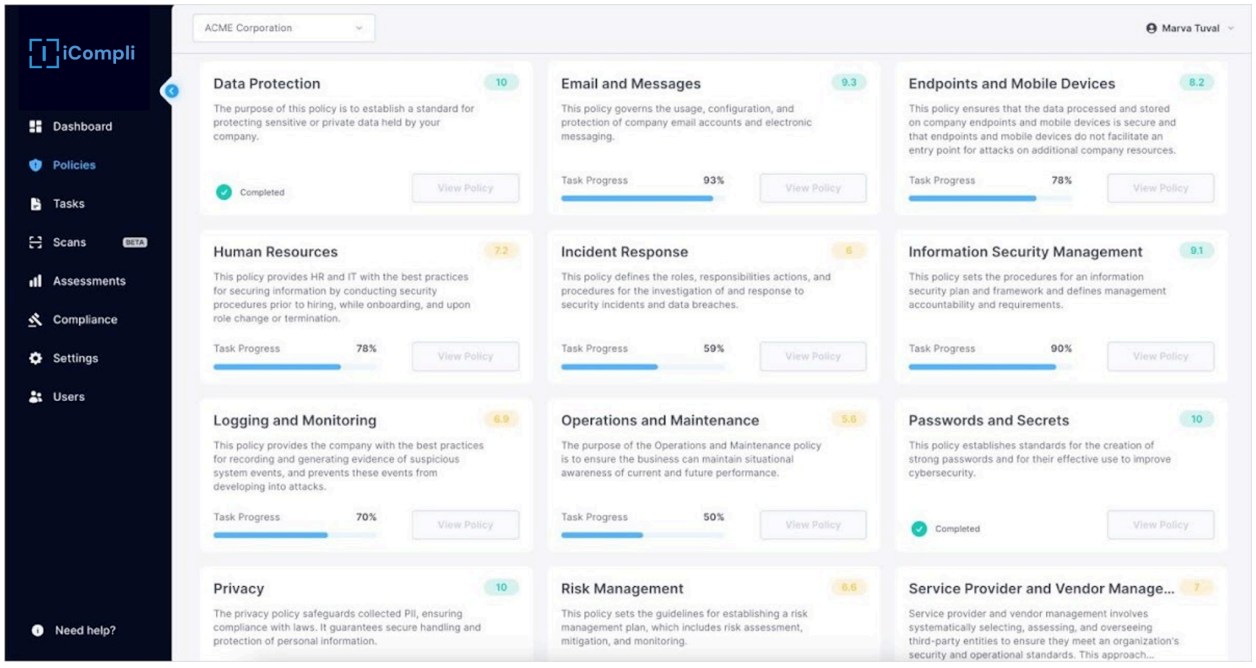
For every client, iCompli produces **a tailored set of security policies** based on industry, risk profile, and regulatory exposure.

These policies are built using our embedded vCISO expertise and written to be practical, clear, and easy to implement.

Within the policy view, users can see:

- **Policy-level security scores**
- **Detailed policy information, including: objectives, scope, and requirements**
- **Linked remediation tasks and completion progress**

Policies can be edited and customized as needed to reflect organizational nuances or client preferences.

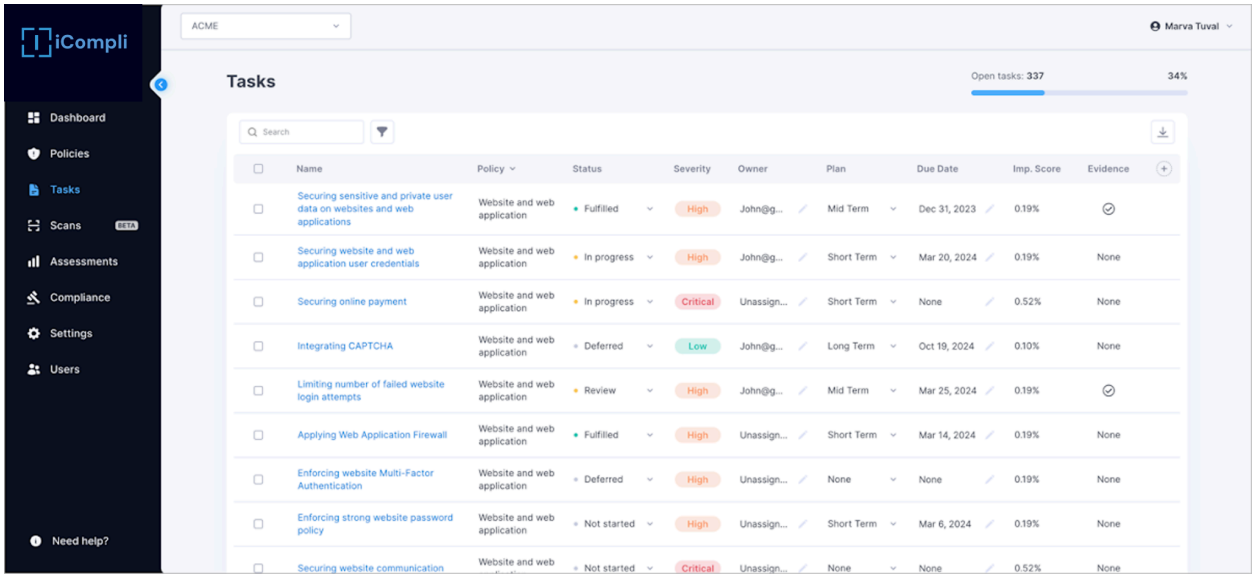


Prioritized, Actionable Remediation Tasks

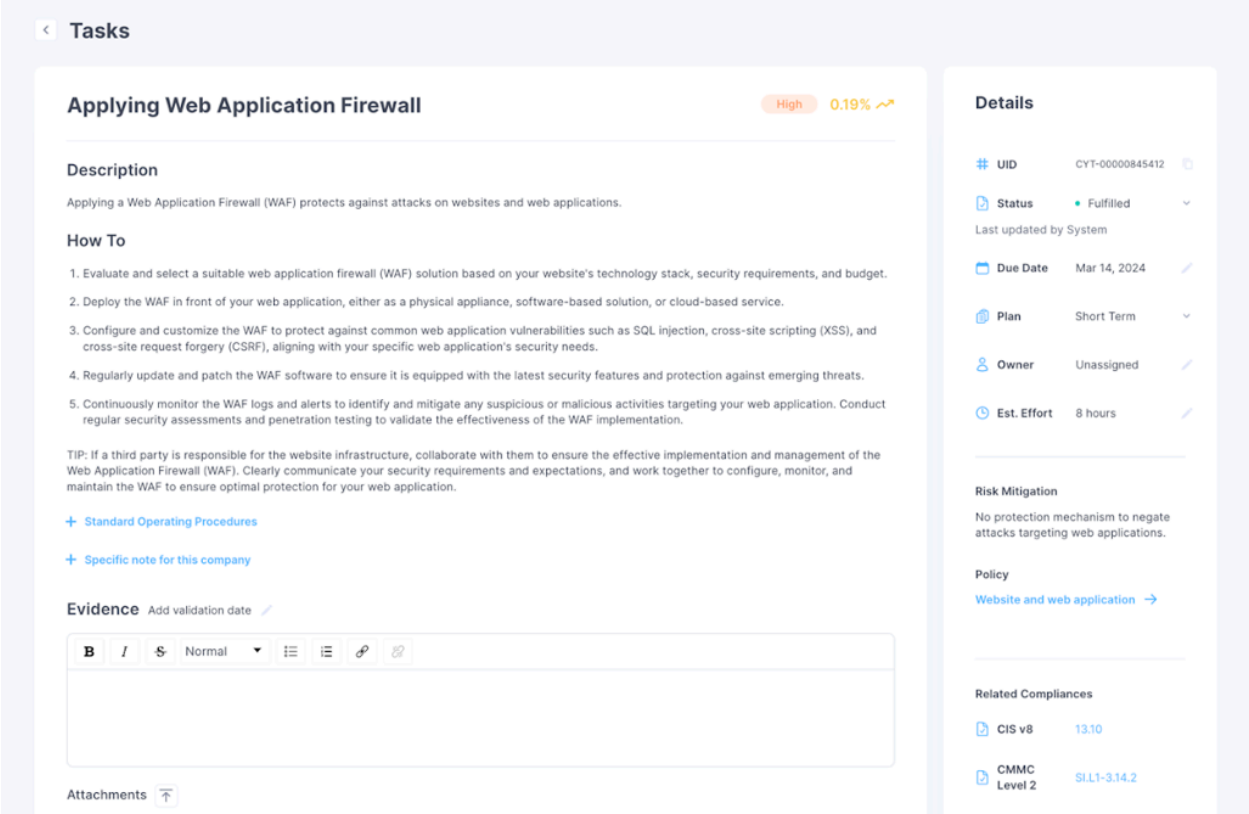
Every policy requirement is automatically translated into **a concrete remediation task**.

Tasks are presented in an AI-generated prioritized list that reflects **severity, risk impact, and current status**. Task categories include:

- **Technical security controls**
- **Administrative and procedural actions**
- **Configuration changes**
- **Operational safeguards**



Tasks can be **modified, deferred, or rescheduled** without distorting overall policy scoring. This allows our vCISO to apply professional judgment while maintaining accurate risk visibility.



Each task includes step-by-step implementation guidance, recommended best practices, and the ability to attach evidence or documentation.

Task completion **automatically updates security scores and compliance readiness** in real time.

Risk Management and Third-Party Risk Oversight

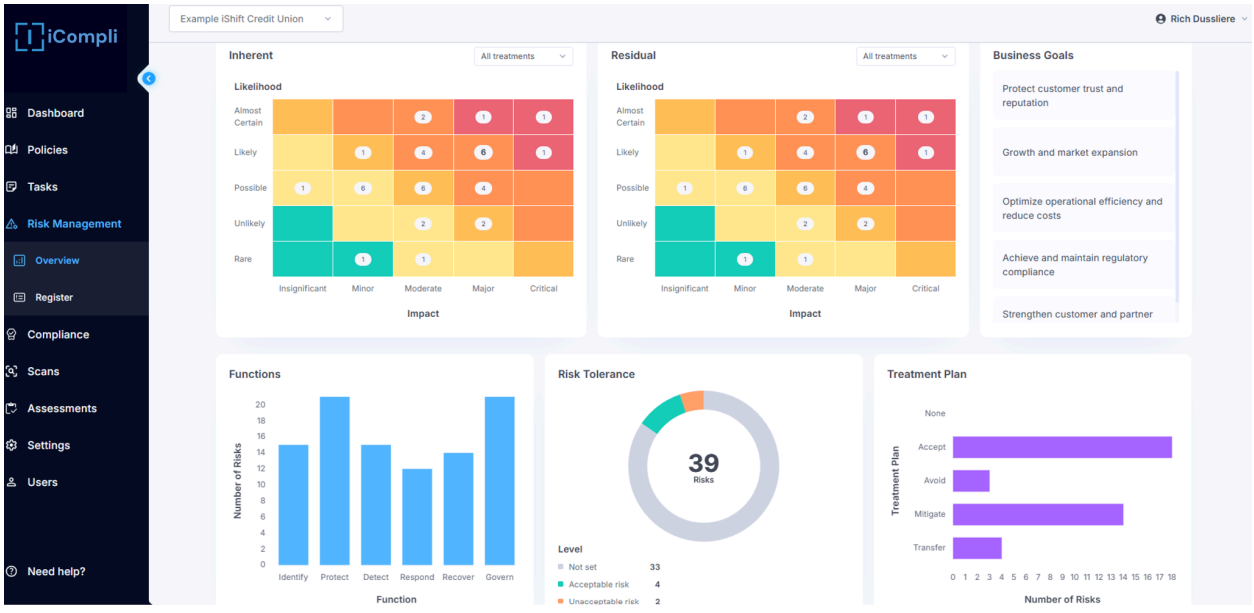
iCompli extends **risk management beyond internal controls** by providing **built-in third-party risk** management capabilities as part of our vCISO workflow. Risk is evaluated in context, connected directly to security posture, compliance requirements, and remediation planning.

Centralized Risk Assessment

iCompli enables structured, repeatable **risk assessments across vendors and business partners**. Questionnaires, impact criteria, and scoring models are standardized and managed from a single platform, eliminating fragmented tools and spreadsheets. Shared vendors can be assessed consistently across multiple clients while preserving client-specific context.

Risk Scoring with Business Context

Each identified risk is evaluated using a standardized scoring model that considers both **likelihood and business impact**. Risks are categorized and visualized using heatmaps, allowing our vCISO to quickly identify high-exposure areas and prioritize mitigation efforts based on what matters most to the organization.

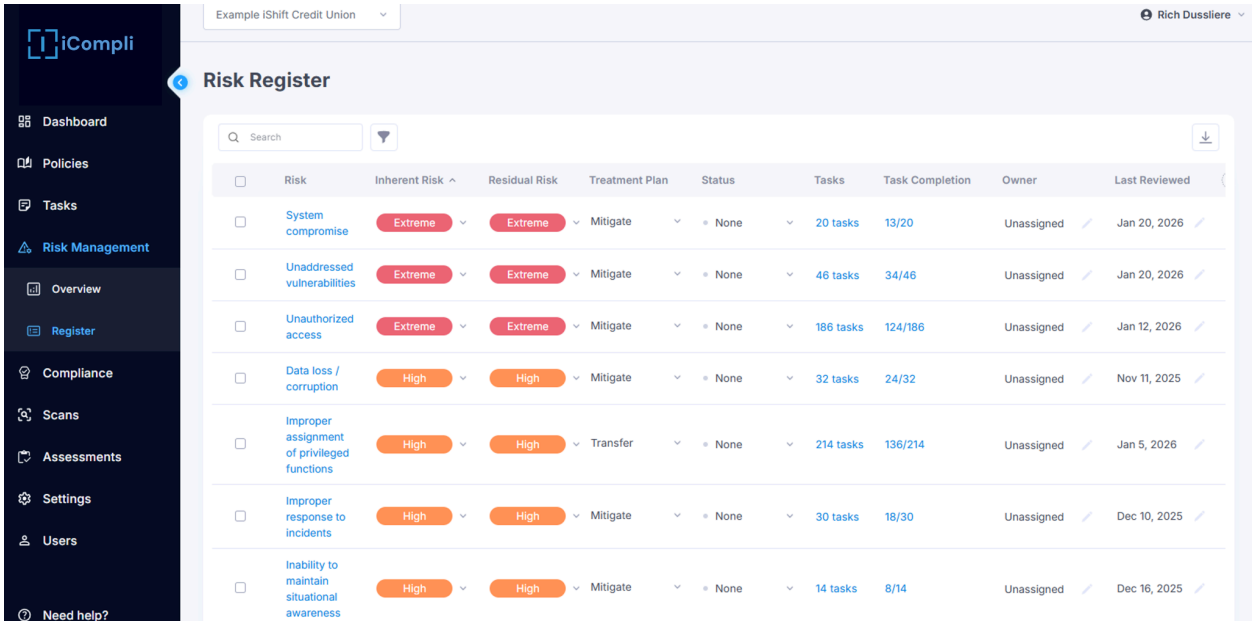


Actionable Risk Visibility

Risk findings are not isolated data points. They are directly linked to relevant security policies, controls, and remediation tasks within iCompli. This ensures that **identified risks immediately translate into concrete actions** rather than static reports.

Automatic Generation of a Risk Register

This capability directly **links risk management to executable tasks** and measures compliance based on the organization's defined risk tolerance. By anchoring both IT operations and compliance teams to the same task-driven workflow, iCompli ensures outcomes are measurable, consistent, and aligned across functions. The approach mirrors how risk professionals evaluate and manage **inherent and residual risk**, aligning naturally with established frameworks such as **NIST AI RMF 1.0, FFIEC, SOC 2, ISO 27001, GDPR, NIST, and CMMC.**



Continuous Monitoring and Reporting

Risk posture is continuously updated as assessments are completed, vendors change, or new information becomes available. iCompli provides **real-time visibility into risk trends across**

vendors and clients, supported by exportable reports that can be shared with leadership, auditors, and regulators.

Turning Risk Insights into Strategic Value

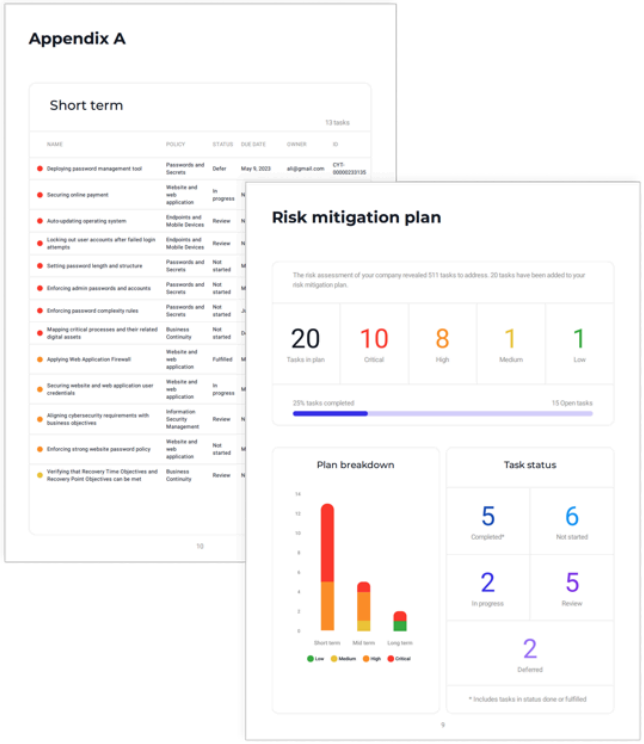
By embedding risk management into our broader vCISO service model, iCompli enables security leaders to **elevate risk conversations from operational findings to strategic decision-making**. Vendor risk insights can be used to support compliance initiatives, strengthen business continuity planning, and identify opportunities for additional security or compliance services.

Planning and Remediation Roadmap

iCompli uses AI to propose an initial remediation roadmap, then provides robust tools to manage execution and progress over time.

Capabilities include:

- **Assigning tasks to short-, mid-, and long-term plans**
- **Scheduling due dates and milestones**
- **Filtering by framework, priority, or status**
- **Editing tasks as requirements evolve**
- **Adding detailed notes, evidence, and recommendations**
- **Associating product or service recommendations to support upsell opportunities**



This **transforms cybersecurity planning into a structured, measurable program** rather than an ad-hoc effort.

Client-Ready Executive Reporting

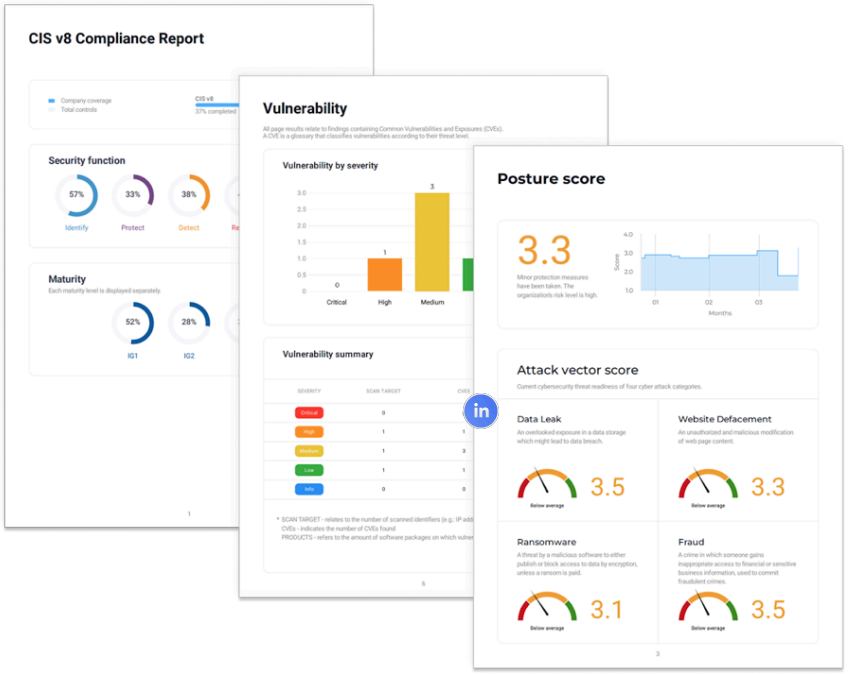
iCompli includes built-in reporting designed for client presentation and **executive review**.

With a single click, reports can be generated to highlight security posture, trends, risks, and compliance gaps relative to industry benchmarks.

Available reports include:

- **Comprehensive Security Report**. A full overview of the organization's cyber posture, remediation progress, and improvement over time.
- **Risk Findings Report**. Focused insight into vulnerabilities and exposures identified through scans.
- **Compliance Readiness Report**. Framework-specific status and gaps.

These reports support meaningful conversations with leadership, IT teams, and stakeholders by clearly demonstrating **risk, progress, and value delivered**.

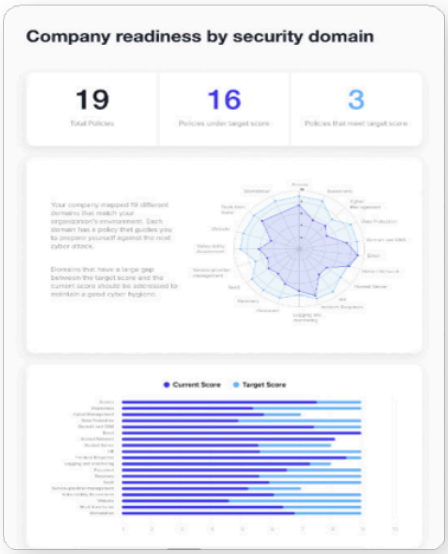


Continuous Improvement by Design

Unlike point-in-time assessment tools, **iCompli operates as a living platform**.

Security scores, compliance readiness, policies, and tasks are continuously updated based on environmental changes, evolving regulations, and emerging threat intelligence. Progress is tracked over time, allowing our vCISO to clearly demonstrate impact and sustained risk reduction.

Turning Cybersecurity into a Business Capability



iCompli is purpose-built to deliver full-spectrum cybersecurity services through a single AI-powered platform.

It enables organizations to **manage security and compliance with the same discipline applied to other critical business functions**. Every task, policy, and control is tied to measurable outcomes, allowing leaders to understand risk, prioritize investments, and clearly communicate progress to stakeholders.

By clearly showing how every action affects risk and regulatory posture, iCompli enables **informed decision-making** and **elevates cybersecurity from a reactive function to a strategic business capability.**

Modernize How Business Works. Securely, Intelligently, Together.

✉ info@ishift.net 🌐 https://www.ishift.net/ in iShift | LinkedIn

🌐 Cybersecurity - iShift