

First AI-Powered Executive Liability Defense Platform Launches with Legal Expert Partnership

Defensibility.ai empowers CISOs and leaders to document compliance decisions and reduce personal liability risks.

NEW YORK, NY, UNITED STATES, October 2, 2025 /EINPresswire.com/ -- As regulators increasingly

“

Executives face rising personal liability. Our platform helps them prove decisions were responsible and defensible in real time, before regulators or boards question them.”

*John Johnson, Founder & CEO,
Defensibility.ai*

target individual executives with personal fines, career-ending bans, and criminal charges, Defensibility.ai today announced the launch of [Defensible Governance™](#)—a comprehensive framework, GenAI platform, and managed legal service built to help executives understand and fulfill their legal governance obligations and defend themselves against personal regulatory scrutiny.

The Defensible Governance™ framework integrates privacy, data protection, cybersecurity, and AI governance laws (including GDPR, the EU AI Act, CCPA, and DORA), crosswalks them to industry standards (ISO, NIST), and

maps them to specific leadership roles—guiding executives to meet both their legal obligations and the standard of "reasonable care" that regulators now demand.

In partnership with privacy and AI law expert [Maverick James](#), Esq., founder of Avant-Garde Legal, Defensibility.ai offers Defensible Governance™ as a managed service combining the GenAI platform with ongoing legal review and validation.

The Shift from Corporate to Personal Liability

Since 2021, authorities have levied more than \$15 billion in penalties globally—many tied to executives' failure to demonstrate reasonable care.

High-profile cases illustrate the new reality:

- Citigroup paid \$336 million in fines across two breaches for failing to demonstrate "reasonable" safeguards
- Uber's Chief Security Officer was criminally convicted for concealment

- Drizly's CEO faces a 20-year personal consent decree
- SolarWinds' CISO was charged by the SEC for alleged security failures

Meanwhile, companies like Marriott and UPMC successfully reduced or avoided fines by proving reasonable governance decisions and documented executive oversight.

"Regulatory enforcement has shifted from just corporate fines to individual accountability," said [John Johnson](#), Founder & CEO of Defensibility.ai

Beyond Compliance Theater

Defensible Governance™ addresses what Johnson calls the "defensibility gap"—the space between proving compliance and proving reasonable care. Traditional governance, risk, and compliance (GRC) platforms were designed to manage controls and pass audits, not to protect individual executives from personal liability. Defensible Governance™ augments existing GRC tools by adding a legal defensibility layer that protects both the company and its executive leaders. The offering is designed to integrate with leading GRC systems like ServiceNow and Drata, with additional integrations planned based on customer needs.

"GRC tools track compliance. We show executives what the law requires of them—and help them prove they met that duty before enforcement hits," said Maverick James, whose firm provides ongoing legal review and validation of the platform's risk assessments.

How Defensible Governance™ Works

The managed service, powered by the Defensible Governance™ platform, includes:

Defensibility Gap Assessment: Evaluates personal and corporate exposure under GDPR, the EU AI Act, SEC cybersecurity rules, and other frameworks to identify where executives lack documented decision-making rationale.

Cross-Regulatory Documentation: Uses unified intake logic for Data Protection Impact Assessments (DPIAs), Fundamental Rights Impact Assessments (FRIAs), AI risk assessments, and SEC disclosures—eliminating duplicative compliance processes. The framework crosswalks regulatory requirements to industry standards like ISO and NIST, while mapping obligations to specific leadership roles.

Legal Test Simulation: Models potential regulatory scrutiny scenarios using enforcement frameworks from the Federal Trade Commission, SEC, and European data protection authorities. The AI engine predicts how specific decisions might be evaluated under regulatory review.

Immutable Audit Records: Generates timestamped, signed documentation of decisions, trade-offs, and risk justifications that can withstand regulatory challenges. Once approved, the system generates and continuously monitors risk mitigation plans.

Role-Specific Dashboards: Provide tailored views for CISOs, General Counsels, CEOs, Data Protection Officers, and boards—each showing relevant duties, exposure, and defensibility status based on the framework's role-mapping methodology.

CYA-as-a-Service: Personal Defensibility Coverage

In addition to the enterprise offering, Defensibility.ai offers CYA-as-a-Service—a private defensibility system built specifically for CISOs, General Counsels, and other senior executives who face personal liability but often lack explicit D&O coverage or indemnification.

The service provides executives with their own audit trail, risk register, and defensibility record, ensuring they can prove diligence and reasonable care before an incident occurs. Features include:

- Personalized Gap Assessment and exposure map.
- Ongoing Updates with risk register entries and defensibility posture.
- Board-Level Exposure Reports that summarize duties, risks, and escalations.
- Confidential Advisory Support from Defensibility.ai and legal counsel during review cycles.
- Private CYA Dashboards accessible only to the executive.

CYA-as-a-Service acts as a structured safety net against regulatory investigations, career damage, or termination without proof of action. For organizations, the service can seamlessly expand into the full Defensible Governance™ offering, providing end-to-end coverage across both personal and enterprise risk management.

Advisory Board Brings Frontline Experience

Defensibility.ai has assembled an advisory board of security executives who have navigated the new regulatory landscape firsthand.

Tim Brown, CISO of SolarWinds, brings critical perspective having faced scrutiny himself. "I've seen how executive decisions can come under intense scrutiny, even when they're made responsibly," Brown said. "Defensible Governance addresses a critical need: helping leaders show the reasonableness of their actions before they're judged in hindsight."

Rich Mason, former Chief Security Officer and CISO of Honeywell, commented:

"Too many CISOs, boards, and executives still believe that compliance checkboxes and 'best effort' will shield them from liability. The reality is different. Prosecutors and regulators systematically reconstruct whether leadership met a reasonable duty of care. We saw this play out in SolarWinds and other landmark cases where compliance alone offered inadequate defense.

Defensible Governance™ is the framework that shifts the balance. It equips leaders to prove, before regulators or in court, that their decisions were reasonable and defensible when they were made. This is no longer optional—it's necessary body armor for managing cyber legal risk."

About Defensibility.ai

Defensibility.ai is the creator of Defensible Governance™, an AI-powered legal defensibility framework and platform focused on executive risk management.

About Avant-Garde Legal

Avant-Garde Legal is a boutique law firm specializing in privacy, cybersecurity, and AI regulation. Founded by Maverick James, Esq., the firm helps organizations navigate complex regulatory compliance requirements and executive risk management in digital governance.

Media Contact:

John Johnson, Founder & CEO, Defensibility.ai

Email: john@defensiblegovernance.com

Maverick James, Esq., Co-Founder & Legal Product Strategist

Email: maverick.james@avant-gardelegal.com

*Defensibility.ai provides tools and guidance to support executive defensibility. It is not a substitute for legal representation and does not guarantee specific legal outcomes.

Maverick James

Avant-Garde Legal

maverick.james@avant-gardelegal.com

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/854591502>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.