

End-to-End Operational Risk Management and Mitigation

Gain actionable intelligence and control via a single Enterprise Risk Management System

Key Benefits



Comply with Evolving Compliance and Data Protection Regulations

Visualize, track, and analyze how personal information is created, collected, used, shared, and disposed across the enterprise to comply with stringent, evolving global privacy, data protection, and security legislation.



Automated and Extensible Impact Assessments

Automate asset inventories, data processing activities, data flow inventories and mappings, security risk assessments, and Data Protection Impact Assessment (DPIA) workflows. Obtain information from your organization on how individual users or teams collect, store, manage, and dispose of regulated information.



Achieve Privacy and Security by Design and by Default

Automate, implement, and monitor the effectiveness of technical controls based on risk analysis from a dedicated system hosted on-premises, in your environment, or in an enterprise-ready private cloud. Ensure security and compliance while incorporating PIAs into your organization.



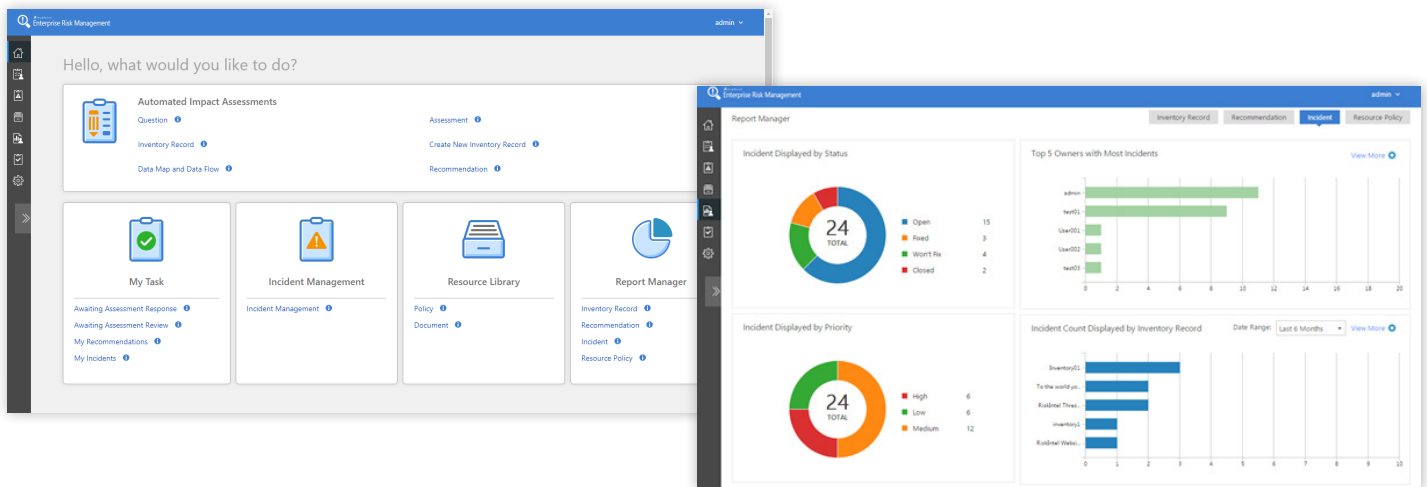
Aggregated and Role-based Reporting

Share the results of your risk registry, data flows, data maps, and impact assessments with executive leadership or data protection authorities and regulators in easily digestible formats. Aggregate responses, export information, and disseminate results with centralized reporting.

Compliance Guardian's Enterprise Risk Management (ERM) is an end-to-end security, privacy incident, and breach management strategy that reflects real-life data protection and risk management within your organization. Create an asset inventory and risk register for data flows across the organization. Comprehensively discover and report on enterprise data. Meet key requirements for global privacy legislation, including the European Union General Data Protection Regulation (GDPR) as well as ISO 27001 and 27002.

Technical Overview

- **Inventory:** Understand your assets and assess risk based on confidentiality, availability and integrity, as well as the sensitive data you hold and how the systems you use collect and protect that data. Assign business impact, PII, and security classifications to data. Integrate with IT Asset Management Systems as necessary.
- **Data Maps & Flows:** Prove that risk-defined data is correctly identified and protected in the authorized systems. Dynamic PII data maps establish and visualize many-to-many associations among IT assets, data subjects, business processes, data handling characteristics, third parties, and jurisdictions.
- **Incident Management:** End-to-end incident management process to capture information, document an incident, prioritize it, determine what's been exposed, or which policies and regulatory requirements are impacted.
- **Privacy & Risk Assessment and Analysis:** Conduct automated Privacy, Risk, Security, and Data Protection Threshold and Impact Assessments with configurable calculators for risk-based decisions and controls. Grant permissions to specific users (local users, Active Directory users, or Windows users) or groups based on responsibilities, with the ability to delegate or reassign response or review tasks.
- **Technical Controls:** Recommend and document appropriate Corrective and Preventive Actions (CAPA) based on non-conformities or other undesirable assessment outcomes. Protect PII and sensitive information with controls for security and compliance, including geography, retention, and classification.
- **Resource Library:** A module designed to centrally manage policies and resource documents related to privacy and security policies – such as GDPR, HIPAA and FISMA – to build an accountable, repeatable process for governance, risk and compliance.
- **Report:** Provide executive reports on Key Performance Indicators (KPIs), Key Control Indicators (KCIs), Key Risk Indicators (KRIs) – including heat maps for sensitive data – to prioritize risk reduction activities, or report on progress made throughout the system, data, individual, and contractual lifecycle.
- **ServiceNow Connection:** Organizations using ServiceNow can sync existing ServiceNow records into ERM as inventory records – or choose whether to sync all records or specific ones matching configured rules.



Carry out repeatable assessments across the entire organization via a centralized dashboard.

For a comprehensive list of new features in this release, please view our [Compliance Guardian Release Notes](#).

How to Buy AvePoint Products

Contact: 201.793.1111 | Sales@AvePoint.com
AvePoint Global Headquarters | 525 Washington Blvd, Suite 1400 | Jersey City, NJ 07310

Start your free trial today:
www.avepoint.com/download