Perform privacy and risk impact assessments via a single Enterprise Risk Management System.

Inventory Manager

- **Inventory Records** – To understand how the data is collected, maintained, disseminated and disposed within your organization, register a data inventory of your organization’s information assets, including the owner of the asset, the business stakeholders, the department and region associated, a description of the recorded applications/services/processes, and more.

- **Risk-defined Data** – Automatically generate risk level and risk score as well as assign security classifications to data to reflect business impact at all levels.

- **Data Assessment** – Apply one or multiple assessments to the recorded inventory and assign them to the corresponding business stakeholders and reviewers to make sure your data is collected and protected appropriately throughout its lifecycle.

- **Data Flow Configuration** – Define the data subject and data element of the inventory record data to enable intuitive data flow and data map.

- **Extensibility with IT Asset Management Systems** – Import and populate data sources in zipped CSV files from your existing IT Asset Management Systems as necessary, or export inventory records individually or in bulk from AvePoint RiskIntel to external regulation authorities for review or book keeping.

- **Inventory Record Recurrence** – Trigger a periodical assessment of the inventory record to ensure your data is secured and compliant with minimum risks.
Privacy Impact Assessment and Privacy Analysis

- **Reusable Surveys** – Create extensive or simple PIAs with ready-made question types, including text, yes/no and multiple choices, and assign them to individuals or teams for response and review.

- **Industry-defined Compliance Assessment** – Adopt a wealth of out-of-the-box questionnaire templates to meet key requirements for global privacy legislation, including the European Union General Data Protection Regulation (GDPR) as well as ISO 27001 and 27002.

- **Branching Logic** – Set up conditional branching questions to create a custom path through the assessment that proceeds flexibly based on a respondent’s answers.

- **Automatic or Manual PIAs** – Generate automatic PIA as part of a software development lifecycle tool via an API call or start it manually to address a specific need.

- **Respondent and Reviewer Delegation** – Delegate or reassign the responsibility for both answering and reviewing questions to appropriate respondents and reviewers during the assessment process.

- **Risk Analysis** – Rate risk scores and risk levels for assessments and inventory records with AvePoint advanced risk calculators and risk matrix mechanism (defined by severity and likelihood) to increase visibility of risks and assist management’s decision-making process.
Corrective and Preventive Actions (CAPA)

- **Risk Recommendation** – Once a risk or non-compliant situation is identified, recommend and document corrective and preventative actions, and improvements, and then delegate a responsible Risk Owner to follow remedial actions to ensure security and compliance.

- **Technical Control** – Protect personally identifiable information (PII) and other sensitive information with appropriate controls, including geography (due to data sovereignty or geo-location restrictions), retention, and classification—reducing risk across the enterprise.

Data Maps and Flows

- **Dynamic PII Data Maps** – Establish and visualize many-to-many associations between IT assets, data subjects, business processes, data handling characteristics, third parties, and jurisdictions, which create the basis for risk analysis based on potential exposure of sensitive data.

- **Intuitive Data Flows** – Keep track of the PII data from the beginning to the end of its lifecycle through intuitive graphic charts that show how the data transfers between data subjects in your organization and prove that risk-defined data is appropriately identified and in the authorized systems.

- **Data Table** – View details of an inventory record including data source, data source location, data subject, data element, data destination and data destination location.
Report Manager

• **Reporting Dashboards** – Leverage filterable dashboards to show ongoing record status, assessment status, risk level, risk growth trend, and incident processing status and priority. Get an overall understanding of the inventory records and their affiliated assessments in your environment, and surface risks that could be detrimental to your organization.

• **Actionable Reports** – Provide executive reports on Key Performance Indicators (KPIs), Key Control Indicators (KCIs), or Key Risk Indicators (KRI) to highlight areas in the organization that need to be addressed to reduce risk, or report on progress made throughout the system, data, individual, and contractual lifecycle.

Status Monitoring and Security Control

• **User Activity Monitoring** – Record all user activities from a security and compliance perspective, including logon/log out, create/edit/delete question/assessments/inventory, respond/review assessments, task delegations, and system setting modifications.

• **Role-based Permission Controls** – Grant appropriate permissions (End User, Record Owner, Record Reviewer, Super User) to specific users (local users, Active Directory users, or Windows users) or groups based on different responsibilities.
AvePoint RiskIntel Out-of-the-Box PIA Templates

- **The Third-Party Vendor Assessment Template** is a collection of sample questions designed to allow a company to build a consistent and repeatable process for managing due diligence procedures for value-added resellers, solutions partners, perpetual referral partners, and all intermediaries that interact with government officials, customers, or investors on an ongoing basis behalf of the company.

- **The Cloud Readiness Assessment Template** is a collection of sample questions designed to help a company understand current data discovery and classification practices and make more informed decisions about readiness for, and migration of data and applications to a cloud provider.

- **The ISO/IEC 27002 Code of Practice for Information Security Controls Template** is an international best practice standard for a set of commonly used information security controls. While none of the controls are mandatory or exhaustive, the standard is commonly used as a cross check, which ensures organizations have not overlooked any important security areas. It is also referenced by ISO 27001, which requires that an organization undertake an information security risk assessment. As part of that process, the template looks to ISO 27002 controls as a basis for risk treatment and to produce a statement of applicability that references the controls chosen for selection based on the organization’s risk appetite. This template is designed to list the controls found in ISO 27002 and turn them into a set of questions that allows security managers to assess any gaps in their control framework.

  **Note:** It is recommended that organizations first perform a risk assessment to determine the applicability of the controls when using ISO/IEC 27002.

- **The ISO/IEC 27001 Information Security Management Template** is the international standard for creating an information security management system. The standard is designed to be a framework and an approach for organizations regardless of size, industry, or location. It aims to ensure an organization has an effective, continually improving management regime that focuses on planning a level of security appropriate to the its legal, regulatory, and contractual requirements. This template takes the requirements of ISO 27001 and transforms them into a set of questions so that organizations, security managers, and auditors can assess themselves or their partners against the requirements for assurance of compliance.

- **The UK Information Commissioner’s Office PIA Template** was created to align with PIA guidance issued by the UK Information Commissioner’s Office.

- **The Singapore PDPC Privacy Impact Assessment Template** was created to align with PIA guidance issued by the Personal Data Protection Commission of Singapore.

- **The Breach Response Template** was created to assess key steps for building a company’s breach response team, and plan and help determine key issues around forensic IT, data, data subject, cyber liability insurance and its communications strategy.

- **The Cyber Security Template** was created to allow a company to assess key elements of its cybersecurity program, from roles and responsibilities to cyber evaluation of hardware, data, encryption and technology, third parties, remote access/BYOD and user accounts/passwords.

For a comprehensive list of new features in this release, please view our [AvePoint Risk Intelligence System Release Notes](https://www.avepoint.com/download).

---

**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](http://www.avepoint.com/download)

© AvePoint, Inc. All rights reserved. AvePoint and the AvePoint logo are trademarks of AvePoint, Inc. All other marks are trademarks of their respective owners.

Accessible content available upon request.