Risk Cloud® Applications

Risk Cloud takes your company's mission-critical governance, risk, and compliance activities to the next level, with a powerful process and workflow management platform that gives you flexibility and accountability while reducing risk.

What are Risk Cloud Applications? We're glad you asked. To put it simply, they were built to help you manage enterprise risk, third-party risk, policy, compliance, data privacy, IT security, and more. Each Application contains all the rules, workflows, logic, and reports you need to run each process, so you can get started quickly.

You have the power to customize Applications to your company's needs and set them up as a stand-alone process in Risk Cloud or linked together for deeper, more holistic insights and visibility on your risks.
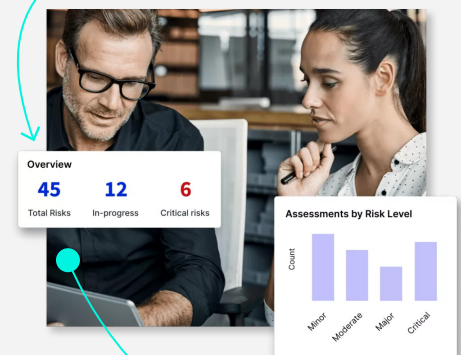
Enterprise Risk Management

Enterprise Risk Management (ERM) Application

Workflows: Risk, Assessments, Mitigations

Description: Build a robust risk register by defining potential risks associated with activities across the enterprise with this Application. Capture everything from vendor interactions and finance, to sales and marketing activity. Create and assign assessments to stakeholders across your business units using the risk register. Track quantitative risk dimensions, such as impact and likelihood, to standardize scoring across the organization and leverage qualitative questionnaires to ensure critical commentary is added to risk data. If risk levels are outside of your organization's acceptable range, log and track risk mitigation activities with the ability to send automatic email reminders to risk owners and mitigation owners.

Frequently Linked Applications: Third-Party Risk Management:SIG Lite, Third-Party Risk Management: ISO 27001, IT Risk Management, Incident Management, Policy and Procedure Management, Issues Management

Enterprise Risk Management: COSO Application

Workflows: Business Objectives, Risk Inventory, Risk Assessments, Risk Responses

Description: Aligned with guidance from COSO's Enterprise Risk Management: Integrating with Strategy and Performance, this Application helps identify enterprise risks and assess risk impact to your strategic objectives. Includes pre-configured risk impact, likelihood, velocity, and vulnerability scoring guidance to help your organization assess inherent risk scoring and residual risk scoring in accordance with response plans. Risk responses can be instantly created and assigned to help your organization further protect strategic initiatives. Automate the creation of risk assessments to your preferred cadence to keep risk owners on track and highlight the enterprise risk landscape.

Frequently Linked Applications: Third-Party Risk Management: SIG Lite, Third-Party Risk Management: ISO 27001, InfoSec Risk Management: ISO 27005, Incident Management, Policy and Procedure Management, Issues Management

Model Risk Management Application

Workflows: Model Inventory, Validations, Findings, Change Requests

Description: Risk Cloud's Model Risk Management Application gives a comprehensive view of all your models to make sure you have the right foundation for assessing financial risk. The models are validated and assigned owners who create and maintain a centralized inventory and perform standardized risk assessments and model validations. Plus, everything is documented in one place where it can be easily reported on and changed.

Frequently Linked Applications: Enterprise Risk Management

Third-Party/Vendor Management

Procurement and Contract Management Application

Workflows: Vendor Repository, Contracts, Service Level Agreements

Description: Ensure the appropriate due diligence is performed before partnering with a new vendor or accepting a new service provider. Representatives from any business unit can submit contract requests to the procurement team via a request portal and manage contracts that are qualified and approved by Procurement before contracting begins. After a contractual relationship is formalized, ensure follow-through of service level agreements with a centralized repository for tracking status and associated due dates. Send automatic notifications to vendor relationship owners when key dates are approaching, such as contract renewal and NDA expiration.

Frequently Linked Applications: Third-Party Risk Management: ISO 27001, Third-Party Risk Management: SIG Lite

Third-Party Risk Management: ISO 27001 Application

Workflows: Third Parties, Third-Party Risk Assessments, Findings

Description: Aligned with ISO 27001's Annex A Information Security Requirements, this application includes pre-built tiering to identify and focus assessment efforts on your data sensitive and business critical third parties. Self-Assessment questions and requested evidence are automatically scoped in or out of the assessment based on the third-party's inherent risk tier. At the end of the self-assessment, each third-party is assigned a risk level based on their self-assessment results. Your organization maintains the ability to instantly create findings and track associated resolution plans within the application.

Frequently Linked Applications: Procurement and Contract Management, Enterprise Risk Management, IT Risk Management, Issues Management

Third-Party Risk Management: SIG Lite Application

Workflows: Third Parties, SIG Lite Assessments, Findings

Description: Leverage your organizations SIG subscription with content aligned with the SIG Lite Questionnaire from Shared Assessments to determine how third parties manage security risks across 18 domains. The Application includes the SIG Lite Business Information Worksheet, Documentation and Artifacts Request List, and all questions from the SIG Lite Questionnaire that allow you to assign and complete forms from your organization's third-party point of contact. Each assessment yields an assessment rating in accordance with the percent of SIG Lite Controls in-place. Instantly create findings, assign finding impacts, and track associated resolution plans through completion.

Frequently Linked Applications: Procurement and Contract Management, Enterprise Risk Management, IT Risk Management, Issues Management

Third-Party Compromise Assessment Application

Workflows: Third Parties, Vulnerabilities, Compromise Impact Assessments

Description: Assess the potential impact of external vulnerabilities or incidents and proactively manage risk by registering third-party relationships, known vulnerabilities, and their potential impact. This Application provides a central register of third-party relationships and details of any identified external vulnerabilities. Using automated workflows, organizations can require completion of compromise impact assessments by their third parties. Once the assessment is completed, the organization can determine if additional action is required to mitigate the potential impact.

Frequently Linked Applications: Third-Party Risk Management: SIG Lite, Third-Party Risk Management: ISO 27001, Enterprise Risk Management, Incident Management, Issues Management

IT Security Risk

IT Risk Management Application

Workflows: IT Assets, Controls, Risks, IT Risk Assessments, Mitigations

Description: Identify critical IT assets across the organization and associate them with logged risks. Customize an inventory of IT risks, including the applicable threat and vulnerability, to centrally track known risks and their assessed risk levels. Leverage pre-defined scoring or configure a unique IT risk assessment methodology and design custom rules based on identified risk ratings. Ensure that users initiate a risk response and create accountability by assigning mitigation activities with due dates to the relevant business or IT owners. As the organization implements controls, users can document the controls in a custom IT controls register or utilize one or more of the control frameworks included in Risk Cloud's control repository, such as NIST 800-53 and ISO 27002.

Frequently Linked Applications: Enterprise Risk Management, Controls Management, Issues Management

Information Security Risk Management: ISO 27005 Application

Workflows: Asset Identification, Risk Assessments, Threat Identification, Vulnerability Identification, Control Identification, Risk Treatments

Description: Identify, assess, and evaluate IT security risks as they relate to organizational IT assets with content that closely aligns with ISO/IEC 27005:2018(E)'s Information Security Risk Management Process to help your organization assess existing threats and vulnerabilities as well as their potential impact on IT assets. Pre-built risk scoring guidance accelerates risk analysis and evaluation and can easily be replaced with your organization's preferred measures. Risk Treatments can be initiated directly from identified risks, assigned to owners, and tracked through resolution to ensure your organization is reducing its overall IT Security Risk footprint.

Frequently Linked Applications: Enterprise Risk Management, Controls Management, Third-Party Risk Management: ISO 27001, Third-Party Risk Management: SIG Lite, Issues Management

Vulnerability Management Application

Workflows: Assets*, Vulnerabilities, Treatments

Description: Automatically ingest vulnerability data including background information, scoring, impacted assets, exploitability details, and more to help manage and assess the vulnerability impact. Use pre-built or custom reports to easily evaluate the status of identified risks and determine which vulnerabilities to fix first. If treatment is required, a treatment record can be initiated, assigned, and tracked through resolution.

This Application can be used in two ways:

- Seamlessly ingest vulnerability data via Risk Cloud Tenable.io Integration
- Leverage the Vulnerability Management Application with a preferred vulnerability sourceor method, such as custom integration or bulk CSV imports.

Frequently Linked Applications: Enterprise Risk Management, Controls Management, SCF Standards and Regulations, HITRUST Standards and Regulations, Issues Management, Incident Management

> *If a customer is using Risk Cloud Tenable.io integration, a full asset listing will be captured in the Vulnerabilities Workflow in an Impacted Assets Text Area instead of the Assets Workflow

Asset Management Application

Workflows: Vendors, Assets, Documents

Description: Know where assets are located, how they are being used, and whether there have been changes made to them with the help of Risk Cloud's Asset Management Application. Track assets related to vendor and document information, like a list of the vendor's internal and external contacts, purchase information, and asset value results, all in one platform. With the help of automated reminders, your stakeholders will automatically be notified when assets are approaching their expected retirement date, or if documents are nearing expiration

In addition, your organization may leverage our ServiceNow integration to seamlessly sync asset information from ServiceNow directly into Risk Cloud. Submit requests for new asset purchases, link documents associated with assets, submit for escalated approval, and monitor expiration dates without having to leave the platform.

Frequently Linked Applications: IT Security Risk Management, Third-Party Risk Management, Procurement and Contract Management, Vulnerability Management

Policy Management

Policy And Procedure Management Application

Workflows: Document Inventory, Document Drafting and Management

Description: Enhance collaboration and improve the quality of policy content across the enterprise with a centralized document repository. Customizable workflows ensure effective and relevant policies, procedures, and other critical documents can be requested, written, updated, and followed by your lines of business. Automatic reminders facilitate the timely completion of policy review and approval requests and enforce periodic update cycles for all key documents.

Frequently Linked Applications: Enterprise Risk Management, Employee Compliance

Compliance Management

Compliance Task Management Application

Workflows: Compliance Areas/Regulations, Compliance Tasks, Task Actions

Description: Comply with compliance requirements by centrally tracking and managing the various regulations, standards, and industry mandates that apply to your business. Set up automatic reminders for recurring tasks, whether annually, semi-annually, quarterly, monthly tasks. Automate due date reminders to the task owner and capture evidence of task completion for easy reference if and when your organization is audited.

Frequently Linked Applications: Issues Management

Employee Compliance Application

Workflows: Employees, Attestations/Certifications, Requirements

Description: Manage the many certifications and attestations that your employees are required to complete by ensuring that your employees have read all of the necessary policies and procedures and completed other important requirements. Build a workflow to help manage and track all upcoming due dates and implement a single source of truth for employee compliance to track employee policy attestations and training requirements to allow for immediate action if an employee is not in compliance.

Frequently Linked Applications: Policy and Procedure Management

SOX Control Testing Application

Workflows: Business Processes, SOX Risks, SOX Controls, SOX Control Tests, Evidence Gathering

Description: Assists teams in maintaining a central repository for all Internal Controls over Financial Reporting (ICFR) by periodic control testing conducted by internal and external auditors to validate the controls are operating effectively and the financial controls yield accurate financial reporting. Conduct Control Tests to ensure the control is adequately designed and has sufficient and clear documentation. Sarbanes-Oxley (SOX) risks can be regularly logged and linked to the appropriate business processes and controls. Document controls,risks and work with Control Owners to keep this information up to date and testing controls on a predefined cadence.

Frequently Linked Applications: Risk Cloud Control Repository, Controls Audit Management, IT Risk Management, Issues Management

See Controls Audit Management section for Controls Management Application

See Regulatory Management section for Regulatory Compliance

SOC 2 Compliance Application

Workflows: SOC 2 Trust Services Criteria, Organizational Controls, Policies, Control, Evaluations, Documentation Requests, Corrective Actions.

Description: SOC 2 is an auditing procedure developed by the American Institute of CPAs (AICPA) to ensure service providers are securely handling, managing, and storing data. Being SOC 2 compliant assures your customers that you have the infrastructure, tools, and processes to protect their information. SOC 2 defines criteria for safeguarding customer data based on five Trust Service Criteria—security, availability, processing integrity, confidentiality, and privacy.

Frequently Linked Applications: HITRUST Controls Management, Controls Management, Enterprise Risk Management

Data Privacy Management

GDPR Compliance Support Applications

Operationalize key requirements outlined in the EU's General Data Protection Regulation (GDPR) by managing personal data. Collect data subject access requests from individuals via a public portal and track the requests through completion. Ensure the appropriate records are kept for all relevant data processing activities. Assess high-risk data processing operations to understand potential risks and implement safeguards as needed. React quickly after a personal data breach occurs to make sure appropriate authorities are notified within the 72 hour required window.

Application: Data Subject Access Request Portal
Workflows: Data Subject Access Requests, Request Confirmation Notifications

Application: Data Processing Activities & DPIAs
Workflows: Assets, Data Processing Activities, Data Protection Impact Assessments

Application: Breach Notification & Management
Workflows: Data Breaches, GDPR Supervisory Authority Notification, Tasks

CCPA Compliance Support Applications

Manage and respond to data handling requests from the California Consumer Privacy Act (CCPA). Workflows address key requirements by utilizing a public request portal to intake requests from consumers. Ensure that all requests are completed within the required 30-day window by enforcing workflow SLAs and due date reminders. Capture key information regarding where personal data is stored and processed within your environment to enable quick execution on consumer rights requests.

Application: Consumer Data Handling Request Portal
Workflows: Consumer Data Handling Requests, Request Confirmation Notifications

Application: Data Processing Activities
**Workflows:** Assets, Data Processing Activities

Incident Management

Incident Management Application

Workflows: Incidents, Response Tasks, and Lessons Learned

Description: Provide a centralized location where incidents reported across the enterprise by employees, customers, or third parties can be logged, triaged, and resolved. Limit risk exposure by immediately addressing known incidents and escalating to the right person. Customize to match incident management within your organization, from the most common to the most complex incident management cases.

Frequently Linked Applications: Enterprise Risk Management, Issues Management, Business Continuity Procedure Tracking
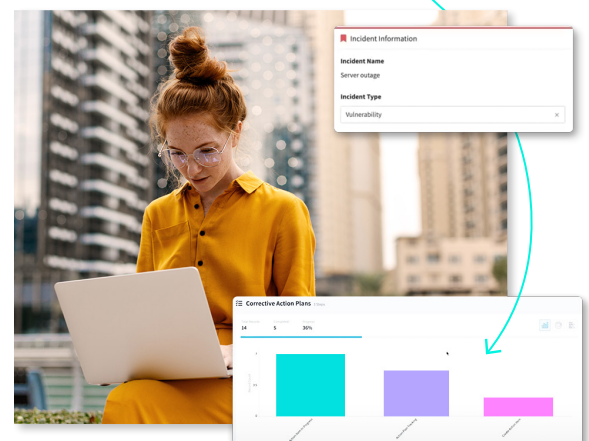
Business Continuity and Incident Response

Business Continuity Plan Management Application

Workflows: Business Continuity Plans, Significant Business Disruptions, Critical Business Functions, Mission Critical Systems, Business Continuity Procedures

Description: Proactively document your business continuity procedures so your organization can continue operating in the event of a major disruption or disaster. Identify the significant business disruptions that may impact your organization. Understand what functions and systems are critical to your business and develop procedures to ensure they are resilient enough to be maintained during a significant business disruption. Once your business continuity plan is built, develop workflows to facilitate the regular testing and updating of your plan to ensure that it continues to accurately reflect what is required to protect your organization.

Frequently Linked Applications: Business Continuity Procedure Tracking, Incident Management, Enterprise Risk Management, Issues Management

Business Continuity Procedure Tracking Application

Workflows: Business Continuity Plans, Significant Business Disruptions, Critical Business Functions, Mission Critical Systems, Business Continuity Procedures

Description: Streamline the execution and tracking of crisis response activities by allowing users to easily capture a Significant Business Disruption (SBD), assign and track tasks that need to be performed in response to the disruption, and create a standard repository of procedures which can be referenced in the event of future disruptions.

Frequently Linked Applications: Business Continuity Plan Management, Incident Management, Enterprise Risk Management, Issues Management

Business Impact Analysis Application

Workflows: Business Processes, Resources, Business Impact Analysis

Description: Aligned with NIST SP 800-34 Rev. 1 guidance and LogicGate's Information Security Team, this Application can identify and prioritize business processes in addition to uncovering necessary resources in the event of a business process failure. Pre-configured forms support the identification of business processes and related resources. Identify outage impacts, estimated downtime, resources requirements, and recovery priorities for resources, including IT systems and assets. Automate the creation and messaging of these analyses to keep business process owners on track and support real-time status reporting to enhance contingency efforts across the business.

Frequently Linked Applications: Business Continuity Procedure Tracking, Enterprise Risk Management, Business Continuity Plan Management, Information Security Risk Management: ISO 27005 Application, Third-Party Risk Management: SIG Lite, Third-Party Risk Management: ISO 27001

Regulatory Compliance

Regulatory Compliance Application

Workflows: Regulations, Obligations, Regulation Risk Assessments, Controls

Description: Identify, track and manage compliance with state, federal, and international laws and regulations required for your organization's operations. Conduct compliance risk assessments to identify inherent risks within your business lines and deploy controls or corrective actions to mitigate identified risks. Be informed of non-compliance to avoid violations that may result in legal punishment, including federal fines.

Frequently Linked Applications: Issues Management, Controls Management, Policy and Procedure Management, Risk Cloud Control Repository

Regulatory Compliance Powered By Ascent Application

Workflows: Profiles, Regulations, Obligations, Risk and Impact Assessments, Corrective Actions

Description: Risk Cloud's Regulatory Compliance Powered By Ascent Application is built from LogicGate's unique partnership between Ascent, a cutting-edge provider of AI-based solutions that automate regulatory compliance.This application enables your organization to continuously assess and monitor regulatory compliance and leverage Ascent's AI technology to deliver relevant obligations specific to your needs. These targeted obligations and rules are automatically scoped to your Risk Cloud environment from Ascent using pre-built Risk Cloud workflows. You can seamlessly assess compliance with obligations scoped for your organization and if compliance gaps are identified, instantly create corrective and preventive action plans.

Frequently Linked Applications: Issues Management, Controls Management, Policy and Procedure Management, Risk Cloud Control Repository

Regulatory Exam Management

Workflows: Exams, Documentation Requests, Findings

Description: Streamline regulatory exam processes across an organization with this Application. Built to support examination owners by providing a central location to document regulatory exams and supporting details to ensure nothing slips through the cracks. Additionally, this Application alleviates the need for examination owners to request documents from owners manually via email. Upon completing the exams, findings can be captured, assigned to owners, and tracked through remediation.

Frequently Linked Applications: Regulatory Compliance, Policy & Procedure Management, Compliance Task Management, Standards & Regulations
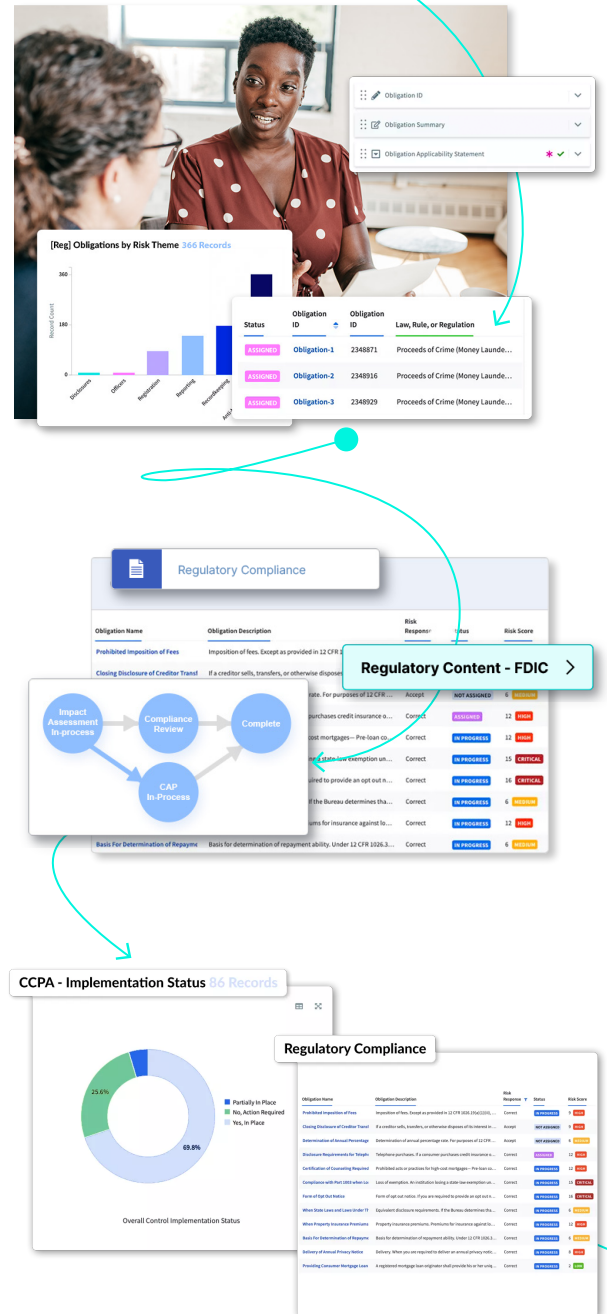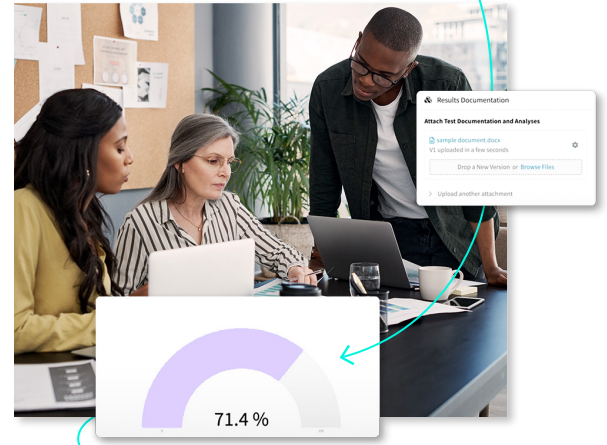
Controls Audit Management & Testing

Controls Management Application

Workflows: Audits, Control Evaluations, Corrective Actions

Description: Link this controls management process template to any control framework, whether from the Risk Cloud Control Repository, an imported control framework, or your organization's custom controls.Facilitate the evaluation of your organization's control effectiveness performing control audits and assigning control evaluations or evidence requests to the appropriate control owners or stakeholders across your business. If control gaps are found, initiate corrective action workflows to ensure steps are taken to address the deficiencies. Expedite your control evaluation processes by utilizing Risk Cloud's linking capabilities to define mappings between various control frameworks so that evaluations or evidence provided for one framework can be viewed and applied for related controls.

Frequently Linked Applications: Risk Cloud Control Repository, IT Risk Management, SOX Controls Testing, Issues Management

HITRUST Controls Management Application

Workflows: HITRUST Assessments, HITRUST Control Evaluations, Corrective Action Plans

Description: Created to support customers with their HITRUST assessment process, the HITRUST Controls Management Application allows users to initiate a readiness, validated, or interim assessment and assign required control evaluations to the appropriate control owner. Control owners maintain the ability to attach control evidence and score controls across all five maturity levels. Evaluation scoring is pre-built within the template and aligns with HITRUST CSF® Control Maturity Scoring Rubrics. Initiate corrective action plans directly from evaluations, assigned to owners, and tracked through resolution to ensure your organization is actively enhancing its information security maturity.

Frequently Linked Applications: Risk Cloud Control Repository, IT Risk Management, Information Security Risk Management: ISO 27005, Issues Management

SOX Controls Testing Application

Workflows: Risk Register, Control Repository, Narrative Repository, Audits, Control Tests

Description: SOX Controls Testing process can be used by internal audit or SOX compliance teams to act as not only a centralized repository for SOX risks, controls, processes, and narrative documents, but also as an effective and simple solution for gathering SOX evidence and housing control testing outcomes. Easily gather test controls in the system through emails to the responsible employee allowing them to quickly drag and drop evidence into the system for review and testing by auditors.

> **NOTE:** This process template does not include time tracking or Gantt charts.

Frequently Linked Applications: Controls Management, Issues Management

Internal Audit Management Application

Workflows: Audit Universe, Operational Risks, Internal Controls, Risk Assessments, Audit File, Audit-Controls Testing, Documentation Requests, Findings

Description: Designed to help Internal Audit Teams achieve operational efficiency and proactively identify gaps by managing and conducting internal audits via the Application. Internal Audit Teams can assess, identify, remediate, and report on issues for internal use and ahead of external audits. Perform control audits and assign work or evidence requests to the appropriate owners or stakeholders across your business. Evaluate and improve the effectiveness of governance, risk management, and control activities to give your organization independent assurance they will meet their strategic objectives.

Frequently Linked Applications: Risk Cloud Control Repository, IT Risk Management, Information Security Risk Management: ISO 27005, Issues Management

CMMC Self-Assessment Application

Workflows: CMMC Practices and Processes, Systems, Evaluations, Remediations

Description: Cybersecurity Maturity Model Certification (CMMC), a government-created framework to measure cybersecurity maturity, is the foundation of the CMMC Self-Assessment Application in Risk Cloud. This Application supports contractors preparing for or seeking to achieve CMMC certification and is built to assess CMMC practice and process effectiveness across your organization and systems. The Application allows for seamless evaluation of the current level of capability of the organization's processes, practices, and methods as well as identify weaknesses and manage remediation efforts aligned with the CMMC framework.

Frequently Linked Applications: SCF Standards and Regulations, HITRUST Standards and Regulations, Issues Management

SOC 2 Compliance Application

Workflows: SOC 2 Trust Services Criteria, Organizational Controls, Policies, Control, Evaluations, Documentation Requests, Corrective Actions.

Description: SOC 2 is an auditing procedure developed by the American Institute of CPAs (AICPA) to ensure service providers are securely handling, managing, and storing data. Being SOC 2 compliant assures your customers that you have the infrastructure, tools, and processes to protect their information. SOC 2 defines criteria for safeguarding customer data based on five Trust Service Criteria—security, availability, processing integrity, confidentiality, and privacy.

Frequently Linked Applications: HITRUST Controls Management, Controls Management, Enterprise Risk Management

SCF Control Assessments Application

Workflows: Assessment File, SCF Domains, SCF Controls, Control Evaluations, Evidence Request, Findings, Additional Frameworks

Description: Risk Cloud's SCF Control Assessments Application is specifically designed to house SCF so that you can assess the maturity of SCF controls and map controls across your risk program. SCF controls can be ingested right into this Application to define your target maturity levels and evaluate your current maturity levels for each control. This streamlined approach means you can reduce resources around your compliance efforts.

Frequently Linked Applications: SCF Standards and Regulations, Enterprise Risk Management, Issues Management, IT Security Risk Management

NIST CSF Assessments Application

Workflows: NIST CSF Controls, NIST CSF Assessments, Control Evaluations, Corrective Action Plans

Description: Seamlessly import the NIST Cybersecurity Framework (CSF) into this Risk Cloud Application and assess your organization's maturity against the NIST CSF Controls to better identify and manage cybersecurity risk. This will also help you to respond to and recover from cybersecurity incidents more effectively. You can instantly initiate and assign corrective action plans and track their progress with the help of automated reminders and contextual messages.

Frequently Linked Applications: SCF Standards and Regulations, Enterprise Risk Management, Issues Management, IT Security Risk Management

Issues Management

Issues Management Application

Workflows: Remediation Action Items

Description: Centralize remediation activities from various sources including audits, assessments, and incidents. As issues are uncovered, document and manage remediation action items via a single Application to reduce the manual and siloed efforts associated with remediation. Coordinate and instantly assign remediation plans to the appropriate owners to resolve issues. Automate in-app and email messaging to keep action item owners on track and support real-time status reporting to enhance remediation visibility across the organization.

Frequently Linked Applications: Controls Management, Enterprise Risk Management, Information Security Risk Management: ISO 27005, Incident Management

Internal Audit

Internal Audit Management Application

Workflows: Audit Universe, Risk Assessments, Audit Plan, Audit Work Programs, Fieldwork, Fieldwork Requirements, Documentation Requests, Audit-Controls Testing, Internal Controls, Findings

Description: Designed to help Internal Audit Teams achieve operational efficiency and proactively identify gaps by managing and conducting internal audits via the Application. Internal Audit Teams can assess, identify, remediate, and report on issues for internal use and ahead of external audits. Perform control audits and assign work or evidence requests to the appropriate owners or stakeholders across your business. Evaluate and improve the effectiveness of governance, risk management, and control activities to give your organization independent assurance they will meet their strategic objectives.

Frequently Linked Applications: Risk Cloud Control Repository, IT Risk Management, Information Security Risk Management: ISO 27005, Issues Management

SOC 2 Compliance Application

Workflows: SOC 2 Trust Services Criteria, Organizational Controls, Policies, Control, Evaluations, Documentation Requests, Corrective Actions.

Description: SOC 2 is an auditing procedure developed by the American Institute of CPAs (AICPA) to ensure service providers are securely handling, managing, and storing data. Being SOC 2 compliant assures your customers that you have the infrastructure, tools, and processes to protect their information. SOC 2 defines criteria for safeguarding customer data based on five Trust Service Criteria—security, availability, processing integrity, confidentiality, and privacy.

Frequently Linked Applications: HITRUST Controls Management, Controls Management, Enterprise Risk Management

SOX Controls Testing Application

Workflows: Risk Register, Control Repository, Narrative Repository, Audits, Control Tests

Description: SOX Controls Testing process can be used by internal audit or SOX compliance teams to act as not only a centralized repository for SOX risks, controls, processes, and narrative documents, but also as an effective and simple solution for gathering SOX evidence and housing control testing outcomes. Easily gather test controls in the system through emails to the responsible employee allowing them to quickly drag and drop evidence into the system for review and testing by auditors.

> **NOTE:** This process template does not include time tracking or Gantt charts.

Frequently Linked Applications: Controls Management, Issues Management

Controls Management Application

Workflows: Audits, Control Evaluations, Corrective Actions

Description: Link this controls management process template to any control framework, whether from the Risk Cloud Control Repository, an imported control framework, or your organization's custom controls. Facilitate the evaluation of your organization's control effectiveness by performing control audits and assigning control evaluations or evidence requests to the appropriate control owners or stakeholders across your business. If control gaps are found, initiate corrective action workflows to ensure steps are taken to address the deficiencies. Expedite your control evaluation processes by utilizing Risk Cloud's linking capabilities to define mappings between various control frameworks so that evaluations or evidence provided for one framework can be viewed and applied for related controls.

Frequently Linked Applications: Risk Cloud Control Repository, IT Risk Management, SOX Controls Testing, Issues Management

Environmental, Social and Governance

Environmental and Social Impact Analysis Application

Workflows: Initiatives, Risks, Benefits, Impact Assessments, Mitigations

Description: Risk Cloud's Environmental and Social Impact Analysis Application supports your holistic ESG program by understanding the social or environmental impact of new projects you are taking on. The Application provides a structure to evaluate environmental and social risks and benefits of each new initiative.

Initiatives are scored to help you quantify their impact so you can make the big decisions. With built-in table and visual reports, dashboards, and automated notifications these insights can easily be communicated to stakeholders.

Frequently Linked Applications: Enterprise Risk Management, Regulatory Compliance, Policy and Procedure Management, Third-Party Risk Management

Mitigation Plan Tracking **36 Records**

Open
Completed
Awaiting Approval
In Progress
Agreed with Mgmt
Under Review

This report summarizes all active Mitigation Plans by Status - can be used as a starting point for Mitigation Plan follow-up

Corporate Social Responsibility Application

Workflows: CSR Strategies, CSR Initiatives, Stakeholder Surveys

Description: You've already established social responsibilities relevant to your mission, operations, and stakeholders. Now you can take action with the help of Risk Cloud's Corporate Social Responsibility (CSR) Application. This Application incorporates seven core subjects from ISO 26000 guidance and uses predefined ratings to determine which core subjects are most relevant to your business. Strategies are made more clear and you can report back to stakeholders through all stages of the social responsibility journey with the help of automated reminders and contextual messaging.

7 Core Subjects:

- Organizational governance
- Human rights
- Labor practices
- Environment
- Fair operating practices
- Consumer issues
- Community involvement and development

Frequently Linked Applications: Environmental and Social Impact Analysis, Incident Management, Policy and Procedure Management, Third-Party Risk Management

Risk Cloud Controls Repository

Risk Cloud's Controls Repository includes controls, requirements, and guidelines from various standards and regulations. For each item listed below, each individual control, requirement, or guideline is stored as a separate object in a repository within Risk Cloud. These individual controls, requirements, or guidelines can then be linked to records in any other process in your Risk Cloud environment, such as policies, enterprise risks, or information security assessments, to name a few.

LogicGate will update the controls repository based on the latest content available for any of the following standards or frameworks:

- Secure Controls Framework
- HITRUST CSF
- ISO 27001
- ISO 27002
- ISO 27018
- ISO 27701
- PCI DSS
- SOC 2 Trust Services Criteria
- NIST 800-53
- NIST 800-171
- FedRAMP
- NIST Cybersecurity Framework
- 23 NYCRR 500
- HIPAA Security Standards (Subpart C)
- GDPR
- CCPA
- CIS Controls Framework
- CMMC: Cybersecurity Maturity Model Certification
- FFIEC CAT
- Australian ISM Guidelines

Request a Demo at
logicgate.com

(312) 279-2775

320 W Ohio St, Suite 5E
Chicago, IL 60654