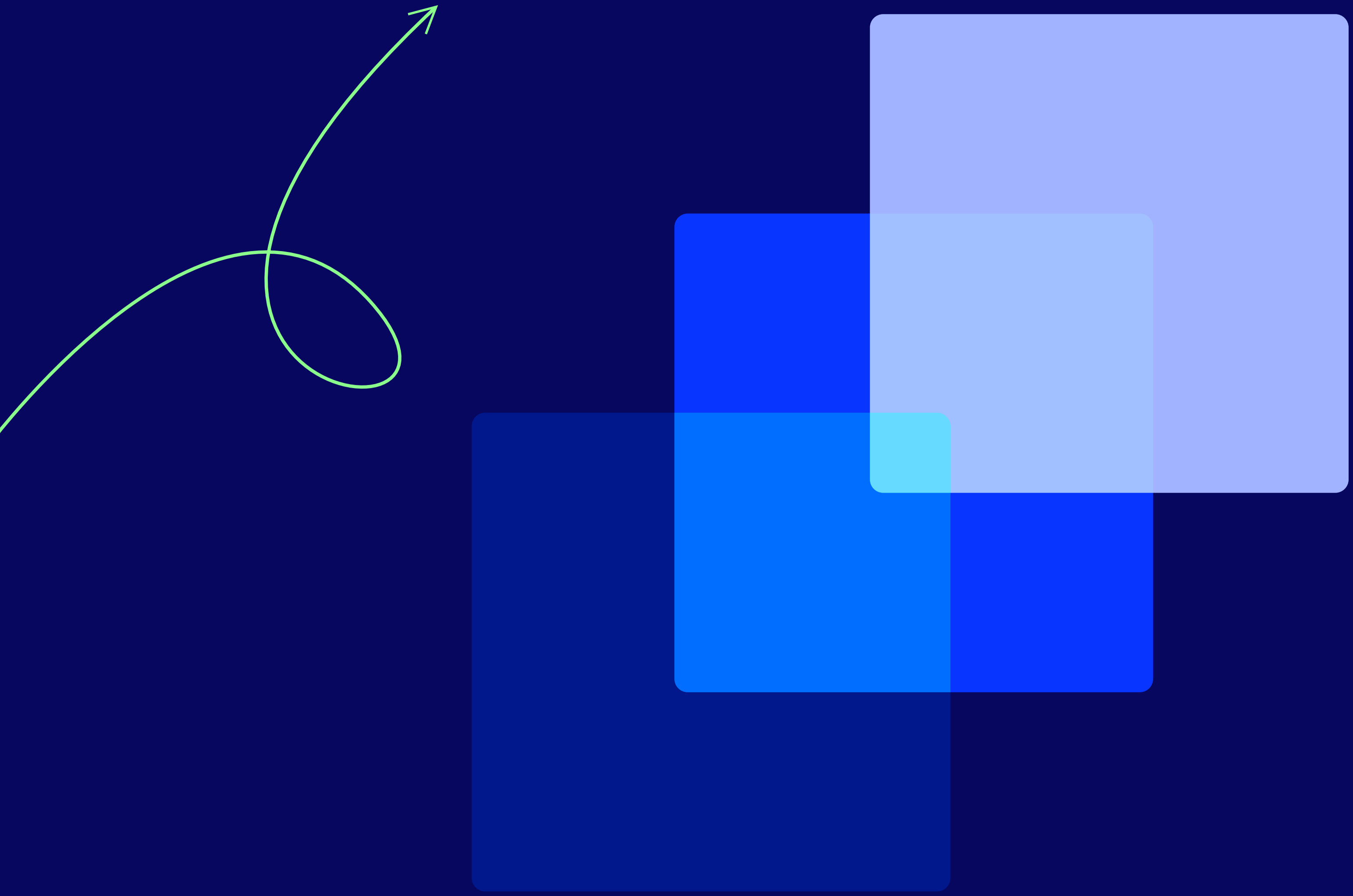
LOGICGATE

How Risk Cloud® Unites Privacy and Security Teams Using One Collaborative Platform



What does it take to build a successful governance, risk, and compliance program today? The simple answer: it requires bringing security and privacy teams together using the right tools to enable better collaboration, communication, and visibility between these two essential departments.

And despite this, too many organizations still treat privacy and security as separate departments, creating a significant challenge for companies lacking visible and collaborative processes for managing data and privacy. Siloed processes and strategies often divide security and privacy teams, resulting in disconnected initiatives, poor communication, and less effective protection. This separation means — even if you comply with every regulation — you still run the risk of being breached if your controls are not configured effectively.

What we know is clear: privacy does not equal security, and security doesn't always translate to compliance. You must go beyond "checking the compliance box" by ensuring your systems are both compliant and secure. And in many cases, this requires collaboration between your security and privacy teams.

What do the numbers say? Gartner estimates that 75% of the global population will have privacy protections by 2024. Meanwhile, security and privacy managers indicate investments in privacy and security build trust with partners and consumers (76% of respondents), mitigate security losses (74%), and enhance operational efficiency (74%). All of these figures make it clear companies must look beyond compliance to truly understand how united privacy and security teams can accelerate company objectives.

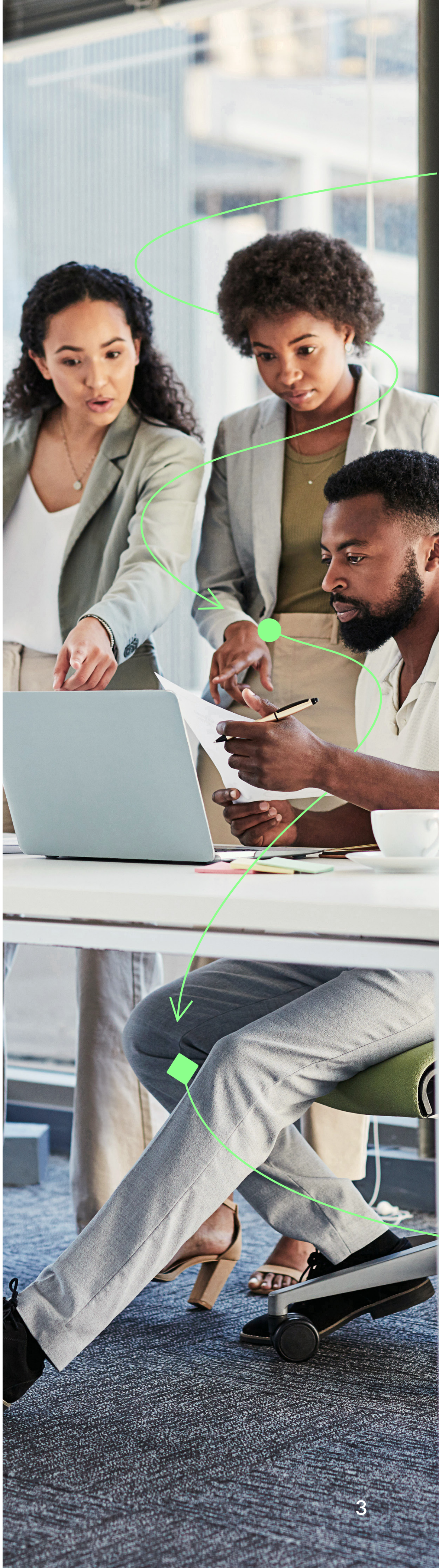
> Security and privacy are both involved in the world of data breaches and compliance. Higher level reporting, cross-mapping controls, and holistic risk monitoring allow these departments to collaborate for the ultimate protection of the entire organization.

So, how can you make security and privacy management a team sport? Keep reading to discover how embracing a holistic approach and using the right platform can unite these teams to achieve compliance, improve your security posture, and unlock a more data-driven decision-making process.

The Common Thread Between Security & Privacy Regulations

As the responsibilities of privacy and security teams evolve to match changing regulatory requirements, realigning teams, goals, and technology is a logical next step. Breaking down silos enhances visibility, collaboration, and execution between these departments and helps organizations with each of the following:

- ISO 27001: This standard focuses on the security of data and related systems. The International Organization for Standardization (ISO) provides a comprehensive framework and organizations must pass a third-party audit to earn an ISO 27001 certification and demonstrate that adequate security controls are in place. Although the certification is not a legal requirement, it's become an industry expectation in healthcare, financial services, and other industries handling sensitive user data.
- GDPR: Any company with customers or clients in the EU must comply with General Data Protection Regulation (GDPR) or face fines of up to €20 million or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. GDPR focuses on the transparent ownership of user data and the responsible and secure use of it. Designed to protect an individual's data rights, users must be allowed to request what information an organization has about them and request to delete data in some situations.
- AICPA TSC (SOC 2): Earning a Service Organization Control (SOC) 2 certification requires implementing specific and effective controls that provide data protection and privacy. Organizations must pass a third-party audit to earn this certification that evaluates confidentiality, user consent, and security controls.
- NIST CSF: The National Institute of Standards and Technology (NIST) developed its Cybersecurity Framework (CSF), initially intended for federal agencies. Yet, it is now freely available for any organization looking to establish or improve its privacy and security posture. While there is no official certification, self-attestation allows organizations to convey how they protect critical systems and sensitive data.
- CCPA: The California Consumer Privacy Act (CCPA) requires businesses to have privacy policies that discuss consumers' data privacy rights and instructs them on how to exercise these rights, including the Right to Know, Right to Delete, Right to Opt-Out of Sale, and Right to Non-Discrimination.



Embracing a holistic, centralized, and connected approach to data privacy and risk management makes achieving compliance and earning certifications significantly more straightforward.

Beyond the frameworks and laws, uniting privacy and security departments creates more effective protection strategies and faster incident response times.

Use Case: Leveraging Risk Cloud to Achieve ISO 27001 Certification

How can you unite your privacy and security departments? Adopting the right GRC platform encourages collaboration and communication between these departments.

> Risk Cloud gives organizations a centralized home for the controls management applications and tools an organization needs to become compliant. Internal controls are brought into Risk Cloud and mapped to multiple frameworks and requirements.
>
> For example, GDPR data processing requirements — including your organization's related processes, assets, controls, and evidence — can map to ISO 27001 requirements via the Secure Controls Framework (SCF) or HITRUST. This capability allows organizations to start with one framework and immediately have a head start on the other.

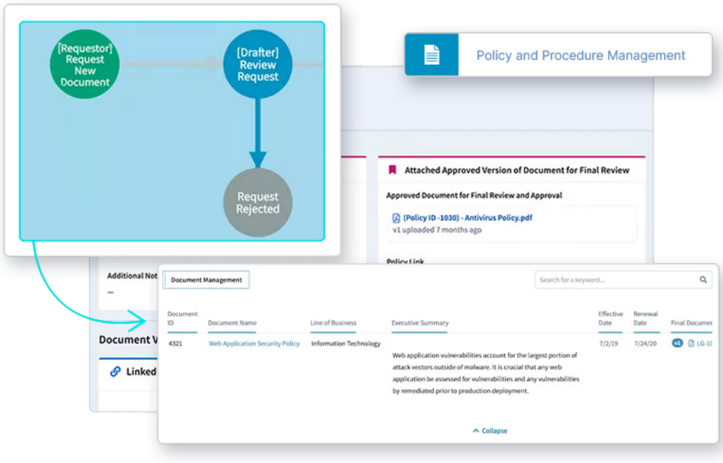
Let's explore how LogicGate's Risk Cloud platform helps you create, manage, and scale essential aspects of your Information Security Management System (ISMS) and GRC program. We'll use ISO 27001 certification as a specific example, but Risk Cloud can also help with the above regulations and certifications.

General Data Protection Regulation (GDPR)
SCF Mappings <> Standards & Regulations
NIST 800-171 Rev. 2 Requirements
NIST 800-53 Rev. 5 Controls
NIST 800-171 Repository
Add Control
NIST 800-53 Rev. 5 Controls
NIST Cybersecurity Framework
☑ Select Data Request Type
* Data Request Type
Data Access
Data Correction
Data Portability
Data Processing Restriction
Data Removal
GDPR Controls
Add Control
GDPR Repository

Documentation, Planning & Security Policy Management

Earning the ISO 27001 certification begins with thorough planning. What systems and data do you need to protect? Do you need to create new policies and processes to protect them? You'll need thorough documentation detailing your security policies — they'll be scrutinized during the audit process.

ISO 27001 requires a specific Information Security Policy document. This document focuses on leadership's commitment to security and details their expectations. Executives won't need detailed information on risk management controls, but the document will provide a high-level overview and indicate executive buy-in.


[Requestor] Request New Document
[Drafter] Review Request
Request Rejected
Policy and Procedure Management
Attached Approved Version of Document for Final Review
Approved Document for Final Review and Approval
(Policy ID -1030) - Antivirus Policy.pdf
v1 uploaded 7 months ago
Policy Link
Additional Not
Document V
Linked
Document Management
Search for a keyword...
Collapse

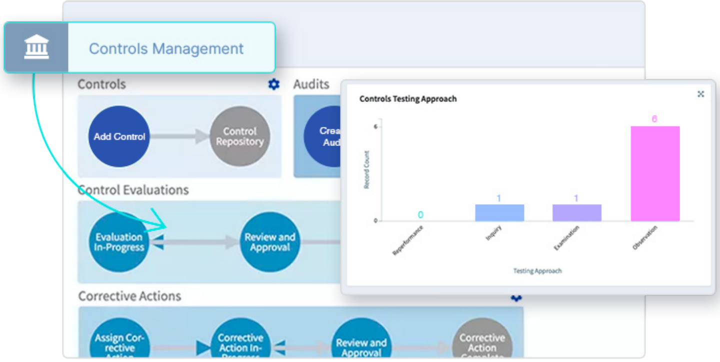
Document ID	Document Name	Line of Business	Executive Summary	Effective Date	Renewal Date	Final Documer
4321	Web Application Security Policy	Information Technology	Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities by remediated prior to production deployment.	7/2/19	7/24/20	v1 LG-1(

How Risk Cloud Helps:

Risk Cloud creates a central home for all ISMS documentation, helping privacy, security, and executives easily find the information they need. In addition, having a central location sidesteps email chains requesting documentation and ensures necessary documents are always up to date.

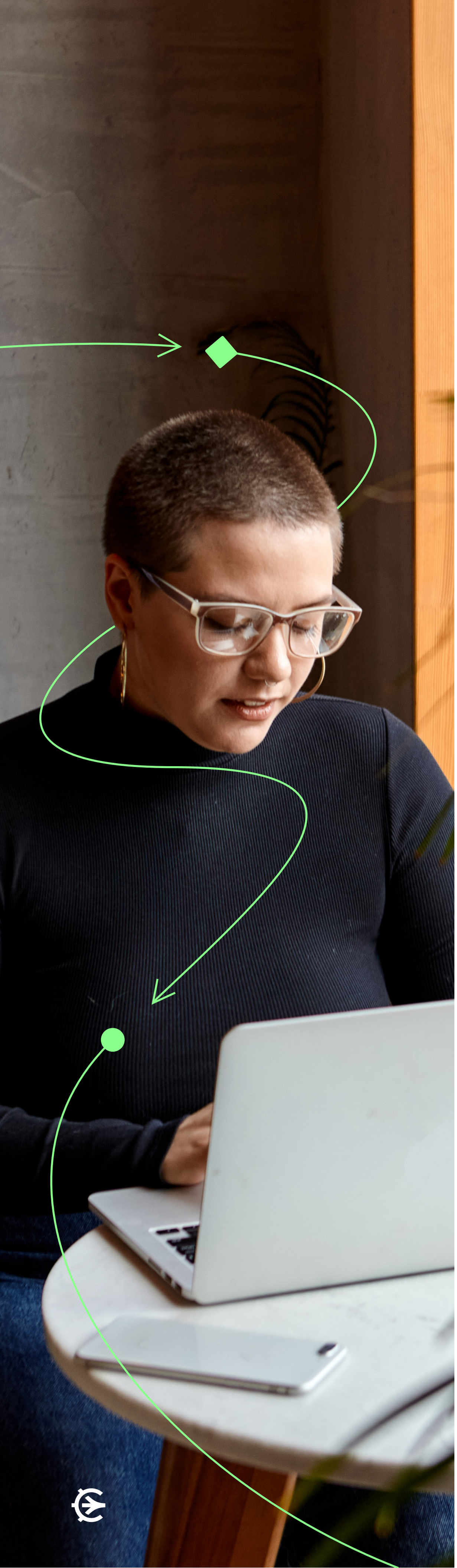
Security Awareness Training Attestation

Employees are your first line of defense but can also be a vulnerability that's exploited. Therefore, ISO 27001 requires security awareness training for all employees and relevant contractors.



How Risk Cloud Helps:

ISO 27001 requires self-attestation about your training programs. Risk Cloud allows you to track training program completion for executives to review and attest. During the audit, your training self-attestation will live in the same location as your other essential documents.



Risk Assessment & Treatment

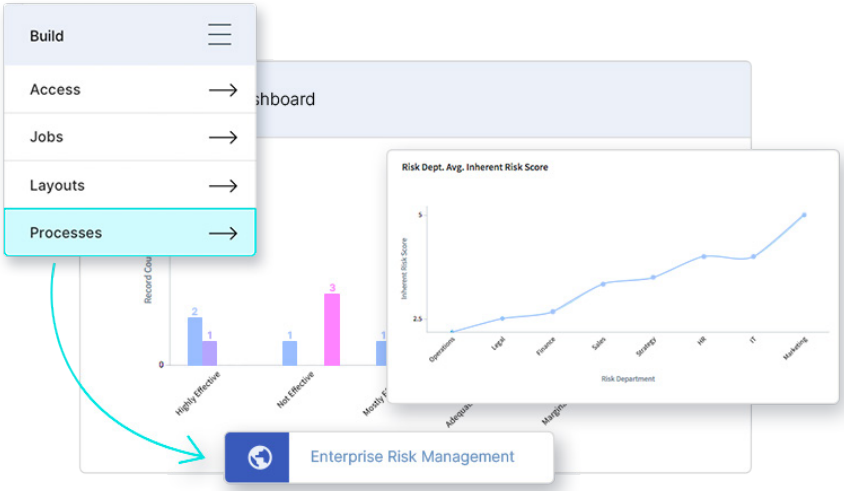
What risks does your company face? What controls have you implemented to mitigate them? How are you monitoring the effectiveness of implemented controls?

The ISO 27001 audit requires detailed answers to each of the above. First, you'll need to conduct a thorough risk assessment and identify every threat facing your business. Then, once identified, determine the potential impact of these risks and prioritize them accordingly.

High-impact risks will require adequate controls, known as risk treatment, and the ISO 27001 framework will inform some controls. Once treated, you'll need to monitor each control to determine its effectiveness continually.

How Risk Cloud Helps:

Risk Cloud helps with every step of the risk assessment and treatment process. Our platform allows you to assess your risk landscape, prioritize known risks, and monitor implemented controls. Both privacy and security teams will be able to view the real-time status of the entire risk management landscape. Additionally, your teams can update the ISMS documentation as necessary throughout the process.

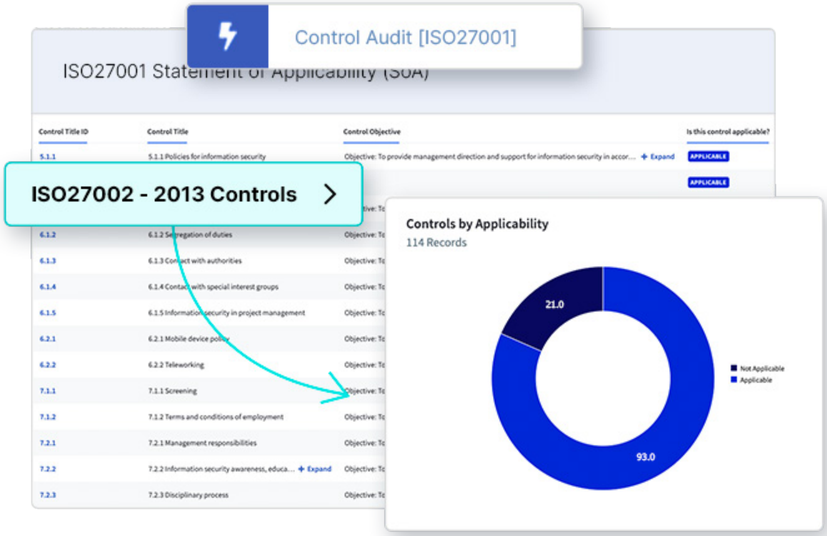


Statement of Applicability (SOA)

The SOA states the specific ISO controls and policies used throughout your organization. This mandatory document will be given to the third-party auditor and your ISMS documents to guide their process.

How Risk Cloud Helps:

Risk Cloud allows you to keep this vital document updated leading up to the audit. Anyone involved in privacy or security will be ready to hand it over to the auditor during the certification process.



Control Audit [ISO27001]

ISO27001 Statement of Applicability (SOA)

Control Title ID	Control Title	Control Objective	Is this control applicable?
5.1.1	5.1.1 Policies for information security	Objective: To provide management direction and support for information security in accor... + Expand	APPLICABLE
			APPLICABLE
		tive: To	
6.1.2	6.1.2 Segregation of duties	Objective: To	
6.1.3	6.1.3 Contact with authorities	Objective: To	
6.1.4	6.1.4 Contact with special interest groups	Objective: To	
6.1.5	6.1.5 Information security in project management	Objective: To	
6.2.1	6.2.1 Mobile device policy	Objective: To	
6.2.2	6.2.2 Teleworking	Objective: To	
7.1.1	7.1.1 Screening	Objective: To	
7.1.2	7.1.2 Terms and conditions of employment	Objective: To	
7.2.1	7.2.1 Management responsibilities	Objective: To	
7.2.2	7.2.2 Information security awareness, educa... + Expand	Objective: To	
7.2.3	7.2.3 Disciplinary process	Objective: To	

ISO27002 - 2013 Controls >

Controls by Applicability

114 Records

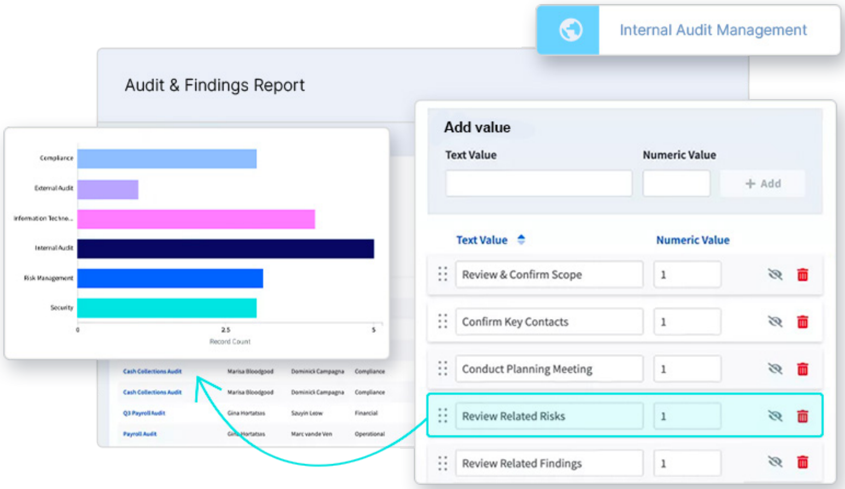
Internal Audits

ISO 27001 requires internal audits at predetermined intervals. Your auditors will need practical working knowledge of the ISO 27001 requirements and an understanding of how a third-party audit is conducted.

The purpose of internal audits is to prepare you for earning the certification and ensure you maintain its requirements afterward. Auditors will ensure the risk management program, and ISMS meet the company's goals and ISO regulatory requirements.

How Risk Cloud Helps:

Risk Cloud simplifies conducting internal audits by providing real-time insights into the entire risk management ecosystem. The auditor will also have access to on-demand reporting to evaluate the historical performance of implemented controls. Additionally, Risk Cloud allows the internal auditor to manage audit documentation, a necessity for maintaining ISO 27001 certification.



Internal Audit Management

Audit & Findings Report

Cash Collections Audit	Marisa Bloodgood	Dominick Campagna	Compliance
Cash Collections Audit	Marisa Bloodgood	Dominick Campagna	Compliance
Q3 Payroll Audit	Gina Hortatsos	Szuyin Leow	Financial
Payroll Audit	Gina Hortatsos	Marc vande Ven	Operational

Add value

Text Value | Numeric Value | + Add

Text Value	Numeric Value
Review & Confirm Scope	1
Confirm Key Contacts	1
Conduct Planning Meeting	1
Review Related Risks	1
Review Related Findings	1

Asset & Vendor Inventory

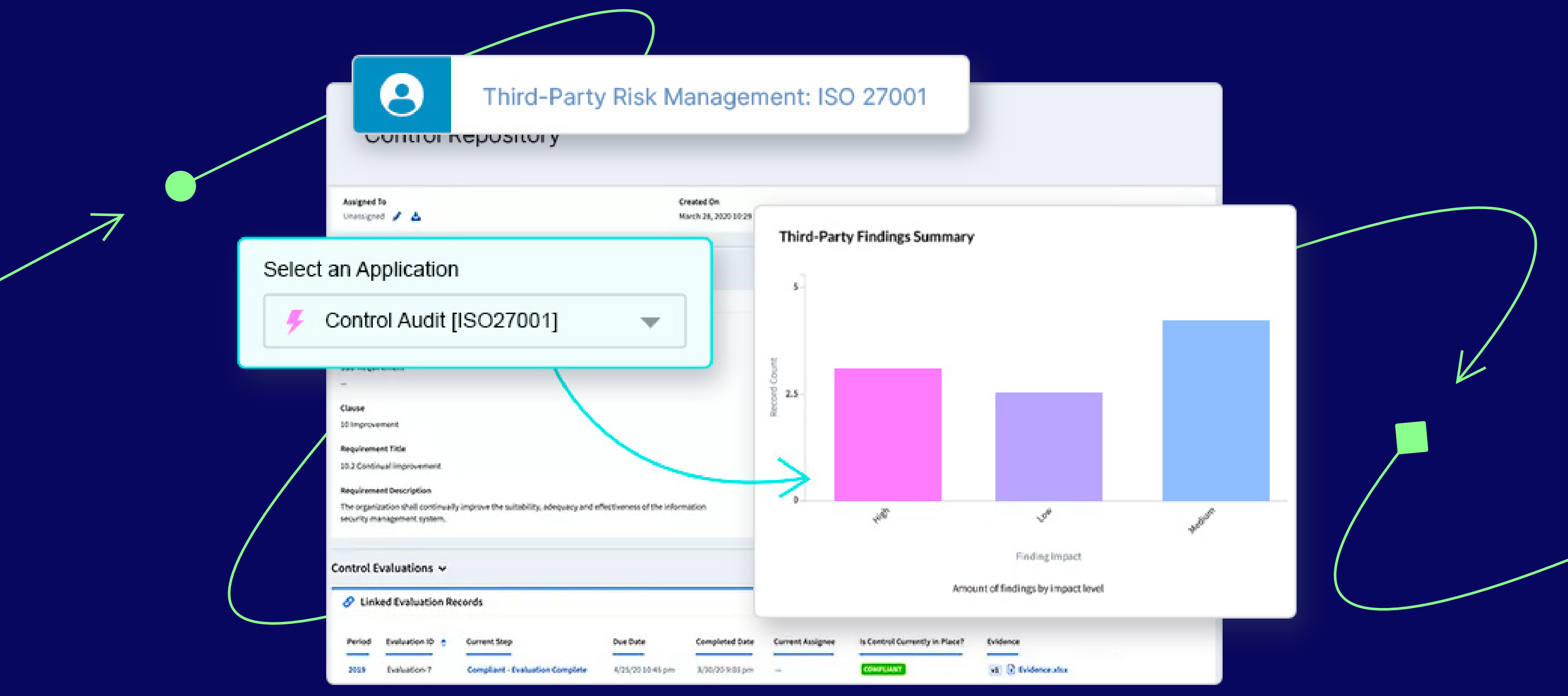
You'll need to create and maintain a comprehensive inventory of risk-related assets covering a wide range of topics. The asset inventory should include:

- Data separated by classification levels and type
- Products or services made available to end users
- Employees, contractors, volunteers, etc.
- Buildings and risk-related physical assets
- Hardware, software, and third-party services

Additionally, each of the above categories also pertains to your vendors. You'll need to document any third-party assets that interact with your assets.

How Risk Cloud Helps:

Risk Cloud gives you the tools to create and update your asset inventory, including those owned by your vendors or partners. Then, your inventory will be readily available during internal and external audits for easy review.



Third-Party Risk Management: ISO 27001

Control Repository

Assigned To: Unassigned

Created On: March 26, 2020 10:29

Select an Application: Control Audit [ISO27001]

Clause: 10 Improvement

Requirement Title: 10.2 Continual improvement

Requirement Description: The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

Control Evaluations

Linked Evaluation Records

Period	Evaluation ID	Current Step	Due Date	Completed Date	Current Assignee	Is Control Currently in Place?	Evidence
2019	Evaluation-7	Compliant - Evaluation Complete	4/25/20 10:45 pm	3/30/20 9:03 pm	—	COMPLIANT	v1 Evidence.xlsx

Third-Party Findings Summary

Amount of findings by impact level

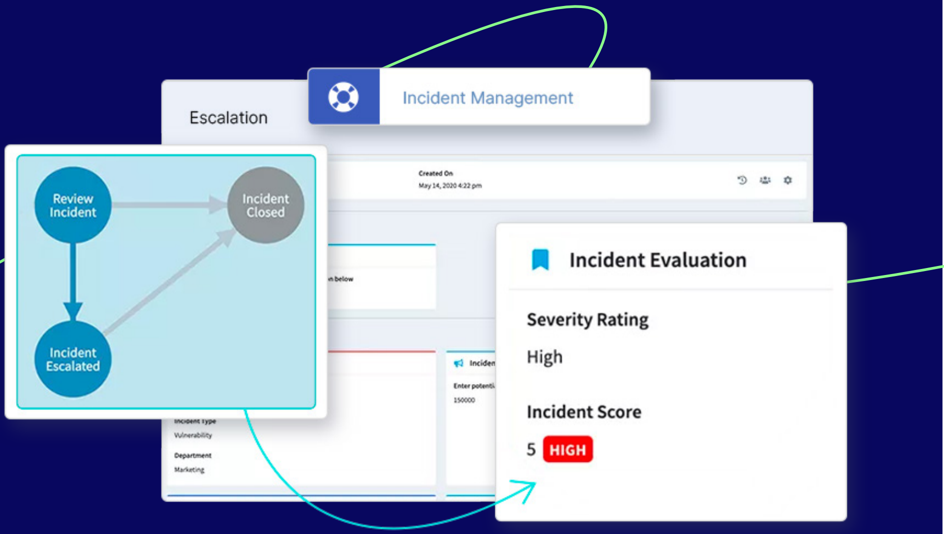
Incidents & Breaches

How will your organization respond to breaches and incidents? ISO 27001 necessitates a thorough incident response program. Your program will detail how privacy and security teams should respond to the given scenario.

Creating an incident response program begins with understanding the risks faced by your organization. Once understood, you'll create documentation that covers what to do if the given risk becomes a reality. Your privacy and security staff will know to follow the plan if an incident occurs rather than trying to figure it out at the moment.

How Risk Cloud Helps:

Risk Cloud allows you to fully understand the enterprise's risk landscape to make sure you create responses to all likely risks. This means your incident response team will be informed and enabled should an incident or breach occur.



Created On
May 14, 2020 4:22 pm

Incident Type
Vulnerability

Department
Marketing

Enter potenti
150000

Severity Rating
High

Incident Score
5 HIGH

Seamlessly Unite Privacy and Security with Risk Cloud

> **Where should you begin?** It depends on your specific needs. When you map your assets to your controls and your controls to risks, it's easy to see how and where security and privacy teams can collaborate and save time.

Uniting privacy and security teams makes achieving compliance and earning certifications easier by breaking down silos and encouraging cross-departmental collaboration. Beyond meeting legal requirements and industry standards, sensitive data and systems will be better protected.

Ready to discover how Risk Cloud can seamlessly unite both teams, enhancing visibility and collaboration in the process? Speak to a risk management expert today and we'll show you why top organizations trust Risk Cloud to create a collaborative process for managing GRC at scale.

About LogicGate

LogicGate is a modern risk optimization company empowering businesses to proactively transform risk enterprise-wide. Because risk is a team sport, we created Risk Cloud® — the most nimble and collaborative GRC platform out there. Rapidly adapt to changing business conditions. Confidently innovate and build new processes as you go. Collaborate on risk across your entire organization. LogicGate's Risk Cloud gives you a truly holistic view of risk that you just can't get from point solutions. After all, great companies are built not by avoiding risks — but by choosing the right ones.

LOGICGATE