RECIPROCITY
rethink compliance.

The Guide to ZenGRC's Compliance Content

ZenGRC offers a centralized registry of content for your organization's governance, risk, and compliance (GRC) activities. We're committed to making your GRC simple and effective; to that end our tool offers the following powerful features to help you reduce complexity when managing your GRC activities:

Common Controls baseline

- We've created a single, baselined set of common information security controls that are mapped to objectives found in the most prevalent security and compliance frameworks including PCI-DSS 3.1, SOC 2, ISO 27001, HIPAA, and NIST SP 800-53 (FedRAMP). Using these common controls, you can easily document your compliance across multiple frameworks/regulations rather than creating compliance documentation specific to each.
- If you're pursuing new certifications or compliance, this mapping eases your task by providing an effortless gap analysis of your current state against the new framework. The mapping shows where your existing controls fulfill the new framework's requirements and allows you to focus on unfulfilled control objectives, reducing the time and effort required to achieve compliance.

Single Source of Truth

ZenGRC offers the ability to consolidate your information security activities by mapping a variety of objects to your information security risk management objectives. This gives you a holistic perspective of your organization's GRC activities and reduces the complexity of managing process, people, and technology across a variety of systems. You can map people, systems, data assets, facilities, regulations, audits, and risks to specific elements of your Information Security Management System (ISMS) or compliance management framework.

For example, you can map firewall configuration objectives to the:

- systems protected
- network engineers responsible for maintenance
- auditors responsible for periodic scans and validation
- data centers where the firewalls are deployed
- relevant regulations those firewalls are subject to, such as PCI-DSS and ISO 27001

This provides your GRC function with a single, collated view of the control objective (proper firewall configuration), its implementation, and ongoing activities to verify that it is operating effectively.

Updated and Verified content

Who has time to stay on top of changing regulations and security frameworks? We do! The team of GRC Experts at Reciprocity stays up-to-date on the latest developments in relevant industry regulation, information security standards, and compliance frameworks. When those change we update the consolidated content and common controls mapping in the ZenGRC database, which is then available for your use in the ZenGRC app.

Standard/ Source	Inventory	Object mappings description	Use case
			CORE Regulations/Standards
SOC2/ SOC3	1 standard 5 sections 116 objectives 169 illustrative controls"	Trust Services Principles and Criteria	SOC 2 objectives are prescriptive; organization may implement their own controls to meet those objectives, or illustrative controls can be implemented if appropriate. Security section is required; organizations may implement other sections (availability, confidentiality, processing integrity, privacy) as needed based on their business. SOC 2 contains 5 principles as of 2016, each featuring standard criteria.
Consolidated Objectives	Varies based on the framework chosen.	SOC 2, PCI, ISO, HIPAA, NIST; Objectives are mapped from one of the frameworks to another, e.g. the 408 objectives in NIST are mapped to the 114 objectivees in ISO 27001/27002.	Maps 5 programs (SOC 2, ISO 27001, HIPAA, NIST, and PCI) at the objective level, to show how existing controls may satisfy objectives in other compliance frameworks. The relationship between controls (mappings) across any of these five programs can be extrapolated using the consolidated objectives. Reciprocity's ""CORE"" frameworks are mapped to assist ZenGRC users understanding of how their controls are mapped accross frameworks.
PCI-DSS v3.1	1 standard 12 Sections 77 objectives 165 controls	PCI-DSS 3.1 Standard	Highly prescriptive, customer control environment needs to align very closely to PCI prescriptive controls and objectives. Difficult to include self assessment, RoC content due to prescriptiveness of standard. Focus on process.
PCI-DSS v3.1	1 standard 35 sections 114 objectives	ISO/IEC 27001: 2013	Medium prescriptive, customer control environment must implement organization-appropriate controls which align to ISO objectives. Encourages more risk-based control with continuous improvement.
NIST SP 800-53 rev4	1 standard 18 sections 408 objectives	NIST rev4	Highly prescriptive, customer control environment typically required to implement all NIST SP 800-53 objectives as part of compliance with US Federal Government requirements.
FedRAMP	1 standard 17 sections 325 objectives related controls	Federal Risk and Authorization Management Program	Highly prescriptive, customer control environment typically required to implement all FedRAMP objectives as part of compliance with US Federal Government requirements. FedRAMP is a subsect, based on NIST 800-rev4.

Standard/ Source	Inventory	Object mappings description	Use case
Common Controls	46 controls	mapped to SOC 2, CSA, ISO, HIPAA, NIST	Turn key control set for enterprise b2b customers. The common control program gives you a baseline set of controls to model your compliance efforts off of. The common controls are mapped to objectives found within SOC 2, CSA, ISO, HIPAA & NIST. Implementing these controls at your organization and adhering to them will enable you to better track your compliance efforts associated with these standards. The common control set is intended for companies who have little or no controls to start with. These are the most nimble controls to use for SaaS based companies. Each common control will require you to customize the language and perform a control walkthrough. These controls are automatically mapped to our consolidated framework.
SOC 1/ SSAE 16/ ISAE 3402	14 control objectives	Suggested objectives and controls for SaaS companies	Not prescriptive, content has suggested control objectives but customer needs to define their own control objectives and controls. SOC 1 does not contain any standardized content since it is based on each company's unique environment. As such, SOC 1 content must be customized for each company, based on existing controls or previous SOC 1 reports.
HIPAA	3 standards 27 sections 275 objectives	1) Security Rule 2) Privacy Rule 3) Breach Notification Rule	Prescriptive guidance for organizations handling PHI; mandatory for organizations defined as a covered entity or covered by a Business Associate Agreement. Contains a mix of controls: required (mandatory), and addressable, which can be implemented via alternate controls or not implemented at all if not appropriate for the organization.
SOX	1 program (reference)	SOX 404	SOX provides highly prescriptive controls and is required for public companies. Focus of the requirements is internal control over financial reporting, specifically focused on documenting such controls and testing their effectiveness.
			Supported Regulations/Standards
COSO	1 standard 5 sections 17 objectives	COSO Framework	Not prescriptive, content is a high level governance framework which provides management with starting points to implement internal controls. Most common use case is for customers interested in SOX, which requires management to implement a controls framework. COSO satisfies this objective.
CSA	1 standard 16 sections 133 objectives	CSA:CCM	Provides prescriptive controls tailored specifically for cloud environments. Build upon common terminology from other information security frameworks. Provides structured means of communicating common information security threats and countermeasures for could providers and cloud consumers.

Standard/ Source	Inventory	Object mappings description	Use case
CSC-CIS/ SANS 20	20 objectives 149 controls		Actionable, prescriptive controls designed to mitgate the Center for Internet Security's top 20 identified informaiton security risks. Not designed to be a complete information security governance or compliance framework, but provides useful prioritization input.
GAPP	1 section 73 objectives	Generally Accepted Privacy Principles	Medium prescriptive, provides a management framework of 10 privacy criteria designed to guide organizations in creating sound privacy practices for dealing with their customer's data.
HITRUST CSF	14 standards 45 sections 149 objectives	HITRUST Common Security Framework	Medium prescriptive framework provides a risk-based control set. Organizations select controls based on a number of factors, including volume of business, geographic scope, regulatory compliance requirements, and system factors.
FISMA	1 workflow 6 tasks	Federal Information Security Management Act of 2002	FISMA establishes compliance requirements related to information risk management for executive and legislative branch agencies of the US Government as well as contractors or vendors supplying them. Requires implementation of controls found in NIST SP 800-53 or FedRAMP. This workflow contains tasks that must be completed to fullfill the requirements of FISMA. This workflow references content for performing a risk assessment, ctaegorizing your system (i.e, high, moderate, low), and selecting the NIST based controls.
ISO/IEC 27017	1 standard	ISO/IEC 27002:2013	Presents medium prescriptive controls for cloud providers and cloud customers. Highlights relevant controls in ISO 27002 with implementation guidance pertinent to cloud hosting and consumption, and provides additional cloud-specific controls.
ISO/IEC 27018 Privacy	1 standard	ISO/IEC 27002:2013	Presents medium prescriptive controls for processing PII in public cloud environments. Highlights relevant controls in ISO 27002 with implementation guidance pertinent to public cloud PII processors.
COBIT 5	5 standards 37 sections 210 objectives	1) Evaluate, Direct and Monitor (EDM) 2) Align, Plan and Organize (APO) 3) Build, Acquire and Implement (BAI) 4) Deliver, Service and Support (DSS) 5) Monitor, Evaluate and Assess (MEA)	Not prescriptive, content is more of an exhaustive framework for governance. COBIT has suggested control objectives but customer needs to define their own controls for aligning to COBIT. COBIT can be used as a framework for SOX.
PCI PIN	7 Sections 33 Objectives 147 Controls	PCI PIN Program	Highly prescriptive controls focused specifically on the secure management, processing, and transmission of PIN data. Integrates with PCI-DSS as part of payment card security.

Standard/ Source	Inventory	Object mappings description	Use case
PCI PTS	6 sections 13 objectives 113 controls	PCI-PTS	Highly prescriptive controls focused specifically on products that process PINs. The program provides modular requirements for Point of Interaction devices where PINs may be captured, processed, or stored.
PCI P2PE	28 Sections 71 objectives 373 controls	mapped to PCI P2PE Program	Highly prescriptive controls to implement Point-to-Point encryption in payment card processing environments. PCI P2PE implementation reduces requirements for compliance of PCI-DSS when implemented properly.
ISMS Template	1 Policy		Reciprocity's ISMS Policy template allows newer compliance teams to build out a set of policies custom to their environment.
FERPA	31 Sections 123 Objectives	Family Educational Rights and Privacy Act	Prescriptive guidance for educational institutions and providers regarding the retention and release of PII. Focuses specifically on educational records and the rights of parents and students regarding privacy and access. FERPA protects the privacy of students' educational records.
WebTrust Principles			Specific to certification authorities. A certification authority is like a house that contains all the keys that decrypt encrypted communications. This standard is a different set of criteria that is narrowly focused on CA activities and there key generation controls.

Need help? Custom content is our speciality!

If your organization has a unique regulatory or compliance requirement, we are available to assist you in documenting that and using ZenGRC to simplify your GRC management. We've helped organizations map to novel frameworks including CNSSI, ISO 27017 & 27018, and Anti-Money Laundering just to name a few. Reach out to us and we'll let you know how we can help.

Reciprocity, Inc.
131 Kissling Street
San Francisco, CA 94103

reciprocitylabs.com
(415) 851-8667
engage@reciprocitylabs.com