Resolver.
A KROLL BUSINESS

Content Packs

The Resolver Core platform supports a growing library of content sources, including operational and technical controls to meet the increasing demands of regulators and auditors. The content packs cover a wide breadth of regulations and standards to establish best-in-industry integration of Governance, Risk, and Compliance.

FFIEC Cybersecurity Assessment Tool
The FFIEC Cybersecurity Assessment is a diagnostic test that helps institutions identify their risk level and determine the maturity of their cybersecurity programs. This content pack includes the FFIEC's Inherent Risk Profile and Cybersecurity Maturity modules. The Inherent Risk Profile reviews 5 key categories: Technology and Connection Types, Delivery Channels, Online/Mobile Products and Technology Services, Organizations Characteristics, and External Threat and is used to determine an institution's overall inherent risk profile across the specific categories. The Cyber Security Maturity module helps institutions assess their maturity levels across the following domains: Cyber Risk Management and Oversight, Threat Intelligence and Collaboration, Cybersecurity Controls, External Dependency Management, Cyber Incident Management and Resilience.

SOC 2
SOC 2 is a framework for intended for service organizations to report information and assurance about controls relevant to security, availability, and integrity of IT systems that process user data and information related to user confidentiality and privacy. SOC 2 defines criteria for managing customer data based on five "trust service principles", and produces reports unique to each organization.

ISO/IEC 27001*
ISO/IEC 27001 (2022) provides organizations with requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System. Implementation can be done by organizations of all types and involve internal and external parties. The requirements of this standard are generic and are intended to be tailored to the needs of the organization.

ISO/IEC 27017*
ISO/IEC 27017 (2015) provides guidelines for information security controls and implementation guidance applicable to the provision and use of cloud services, for both providers and customers. This framework includes additional controls specifically related to cloud services and implementation guidance for relevant controls specified in ISO/IEC 27002.

ISO/IEC 27018*
ISO/IEC 27018 (2019) focuses on protecting personal data in the cloud. In addition to new privacy controls in Annex A, it also provides implementation guidance on ISO 27002 controls applicable to personally identifiable information (PII) in the cloud.

ISO 27799*
ISO 27799 (2016) is intended to be used in accordance with ISO 27002 to help healthcare organizations manage health information security by providing health information security best practice guidelines. By implementing these guidelines, healthcare organizations can ensure the personal health information is at a minimum level of security that is appropriate for their organization.

ISO/IEC 27002*
ISO/IEC 27002:2022 is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC 20000-1*
ISO/IEC 20000-1 (2018) provides specific requirements for establishing, maintaining, and continually improving a service management system, including guidance on the application of service management systems and examples of how to meet the requirements.

ISO 9001*
ISO 9001 (2015) promotes the adoption of a process approach when developing, implementing and improving the effectiveness of a quality management system in order to enhance customer satisfaction by meeting customer requirements.

ISO 22301
ISO 22301:2019 is an international standard for business continuity, helping organizations prepare for and recover from disruptions, ensuring critical operations continue during emergencies.

*ISO content available in certain regions only

NIST CSF 2.0

The NIST Framework for Improving Critical Infrastructure Cybersecurity focuses on using business drivers to guide cybersecurity activities and consider cybersecurity risks as part of the organization's risk management processes. Organizations of all sizes, degrees of cybersecurity risk, or cybersecurity sophistication, are able to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure using this framework.

FedRAMP

The Federal Risk and Authorization Management Program is a United States federal government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

NIST Privacy

This publication describes the voluntary NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Version 1.0). The Privacy Framework is a tool developed to help organizations identify and manage privacy risks to build innovative products and services while protecting the privacy of individuals. The Privacy Framework provides a flexible, risk- and outcome-based approach, intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction. The Privacy Framework follows the structure of the NIST Cybersecurity Framework to facilitate the use of both frameworks together.

NIST 800-53

The purpose of the NIST 800-53 Rev. 5 publication is to provide a complete approach to information security and risk management by providing organizations with the security controls necessary to fundamentally strengthen their information systems and their operating environments. The security and privacy controls have been designed to be largely policy/technology-neutral to facilitate flexibility in implementation. This content pack contains the most recent NIST 800-53 Rev. 5 update and supplementary document NIST 800-53 Rev. 5 to address the increasing sophistication of cyberattacks.

NIST 800-171

NIST 800-171 Rev. 3 provides recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal systems and organizations. These requirements apply to all components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.

PCI DSS 4.0

The PCI Data Security Standard (PCI DSS) is a global standard that establishes a baseline of technical and operational requirements to protect payment data. PCI DSS 4.0 represents the next evolution of the standard, developed through global industry collaboration.

CMMC

The Cybersecurity Maturity Model Certification (CMMC) framework consists of maturity processes and cybersecurity best practices from multiple standards, frameworks, and other references, as well as inputs from the Defense Industrial Base and Department of Defense stakeholders.

HIPAA

The Health Insurance Portability and Accountability Act (effective April 14, 2003) is a US law designed to impose privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. Developed by the Department of Health and Human Services, these standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this new rule.

Privacy Legislations

GDPR

The General Data Protection Regulation (GDPR) is an EU law that regulates the collection, use, and storage of personal data, ensuring the privacy and rights of individuals. It applies to organizations inside and outside the EU handling EU residents' data.

PIPEDA

PIPEDA is Canada's privacy law that governs how organizations collect, use, and disclose personal information in commercial activities, requiring consent and safeguarding data privacy.

CCPA

The California Consumer Privacy Act (CCPA) gives California residents rights over their personal data, allowing them to know, delete, and opt out of the sale of their information. It applies to certain businesses based on revenue or data handling thresholds.

*ISO content available in certain regions only

Framework Enhancements

Resolver.
A KROLL BUSINESS

Framework enhancements are additional developments that provide depth to our framework offerings and are automatically included with framework subscriptions. These enhancements are unique to Resolver, and were included to enhance customers' compliance efforts and effectiveness.

Framework Content Mappings

Organizations often utilize multiple frameworks to guide their cybersecurity strategy and certification goals. Quite often, there are significant overlaps in evidence and controls between frameworks. Framework mappings are leveraged to draw connections between these overlaps and allow customers to easily document their compliance across multiple frameworks rather than creating compliance documentation specific to each one. These mappings show where existing controls may fulfill new framework requirements and allows companies to focus and consolidate their efforts while offering a single source of truth.

Framework Mappings we offer:

- FFIEC: NIST CSF 2.0
- FFIEC: PCI DSS 4.0
- PCI DSS 4.0: NIST CSF 2.0
- PCI DSS 4.0: ISO 27001 (2022)
- SOC 2: ISO 27001 (2022)
- SOC 2: PCI DSS 4.0
- SOC 2: NIST 800-53 rev. 5
- SOC 2: NIST CSF 1.1
- SOC 2: NIST CSF 2.0
- ISO 27001 (2013): ISO 27001 (2022)
- ISO 27001 (2022): NIST CSF 2.0
- NIST 800-53 rev. 5: ISO 27001(2022)
- NIST 800-53 rev. 5: NIST CSF 2.0
- NIST 800-171 rev. 3: NIST 800 171 rev. 2
- NIST 800-171 rev. 2: PCI DSS 4.0
- NIST CSF 1.1: NIST 800-53 rev. 5
- NIST CSF 1.1: ISO 27001(2022)
- NIST CSF 1.1: SOC 2
- NISF CSF 1.1: NIST CSF v2.0
- NIST CSF 2.0 - FFIEC
- NIST CSF 2.0 - NIST 800-53 rev. 5
- NIST CSF 2.0 - PCI DSS 4.0
- NIST CSF 2.0 - SOC 2
- NIST CSF 2.0 - ISO 27001(2022)

Want to learn more? Let's talk.

resolver.com | info@resolver.com | 1-888-316-6747 | See Risk. Build Resilience.