


Key Considerations of a Data Protection, Information Risk Management and Compliance Program

Effectively managing data, information risk and compliance is complex and ever-changing. There are many components and considerations in developing and implementing a robust program that encompasses and integrates all the elements needed to manage this risk and achieve one's compliance objectives effectively. Many organizations believe selecting their information risk management framework is the most complicated part of the process, and although important, it is just the beginning.



What questions should we be asking regarding our data protection, information risk management and compliance program?

How do we identify, evaluate and implement an assessment tool that can support our framework, catalog threats and inherit cloud and business outsourced controls?

How do we measure the effectiveness of implementing and operating privacy and security controls based on our framework?

How do we identify a framework that is comprehensive and addresses our regulatory, risk and third-party requirements as it relates to privacy and security?

How can we systematically and with transparency track our third parties, especially those with PII and PHI, to ensure that they have implemented appropriate privacy and security controls?

What's the most effective way to provide assurance from a third-party review on our controls that senior management, regulators and customers will consider as valid and acceptable?

What are our due diligence and due care obligations for information risk management?

Are we addressing applicable state, federal and international regulations?

How do we ensure that the controls leveraged by cloud service providers are mutually understood and evaluated appropriately?

What metrics are we using to measure ourselves against comparable organizations?

How do we integrate information risk management into an enterprise risk management program?

How do we reduce our cybersecurity insurance premiums?

How do we provide comfort to senior management and the board on our organization's security and privacy posture by leveraging an industry recognized standard?

How do we select a program and tools that scale within our organization and align with our risk profile and assessment?

In developing an information risk and compliance program, there are many considerations in addition to selecting the most appropriate framework:

- Aligning threats to security controls
- Reporting your program's approach to management and third parties
- Integrating information risk and compliance controls into an assessment tool
- Measuring the effectiveness of implementation
- Sharing control responsibilities with service providers
- Aligning with a third-party risk management approach

HITRUST Approach to Information Risk Management and Compliance

HITRUST understands information risk management and compliance and the challenges of assembling and maintaining the many and varied programs, which is why our integrated approach ensures the components are aligned, maintained and comprehensive to support an organization's information risk management and compliance program.

Designed to leverage the best in class components for a comprehensive information risk management and compliance program that integrates and aligns the following:

HITRUST CSF®—a robust privacy and security controls framework

HITRUST Threat Catalogue™—a list of reasonably anticipated threats mapped to specific HITRUST CSF controls

HITRUST MyCSF®—an assessment and corrective action plan management platform

HITRUST Assessment XChange™—an automated means of sharing assurances between organizations



HITRUST CSF Assurance Program—a scalable and transparent means to provide reliable assurances to internal and external stakeholders

HITRUST Shared Responsibility Program—a matrix of HITRUST CSF requirements identifying service provider and customer responsibilities

HITRUST® Third-Party Assurance Program—a third-party risk management process

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net