THE 19 HITRUST DOMAINS

A Comprehensive Approach to Information Security

BARR ADVISORY

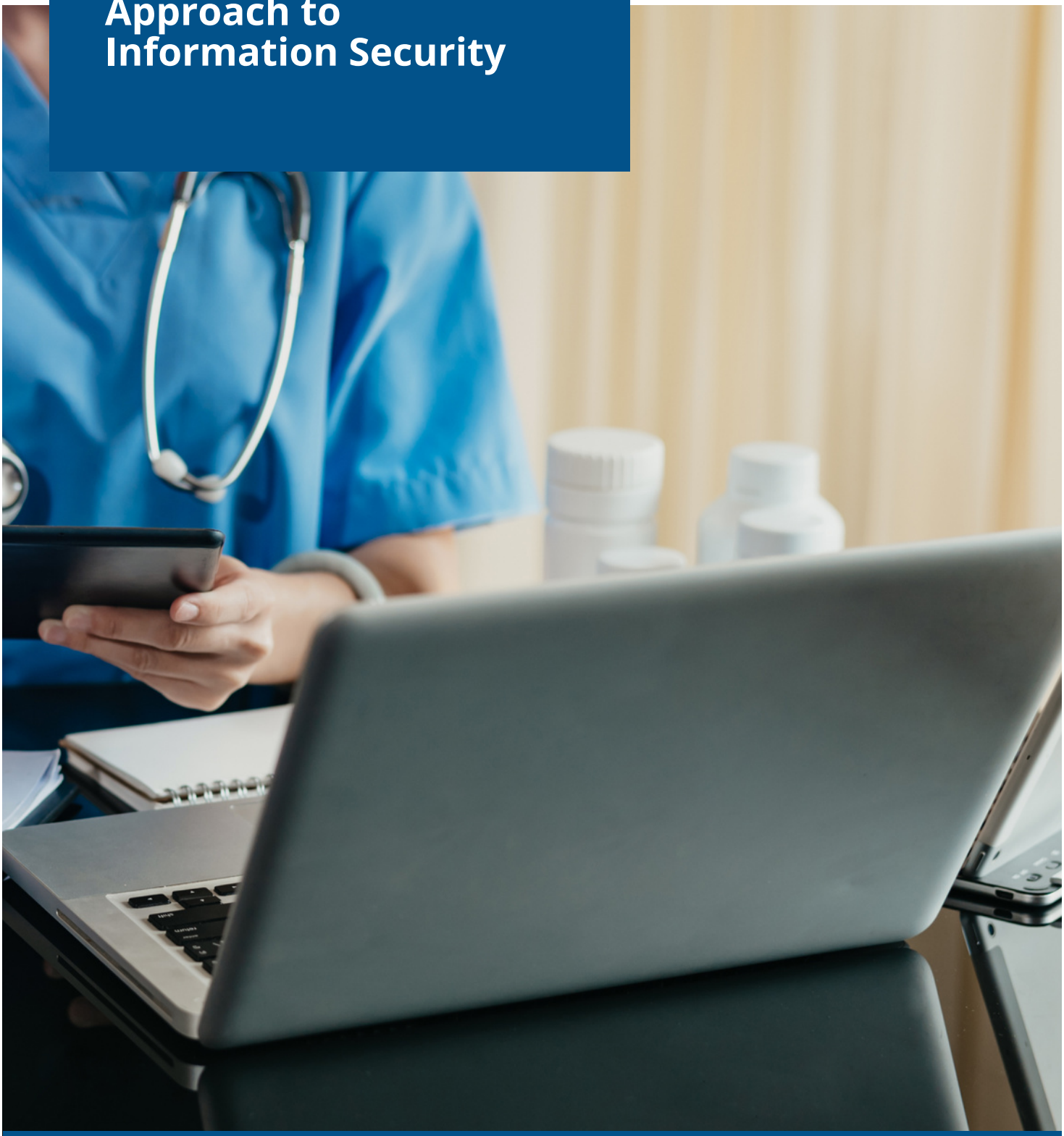

Table of Contents

Introduction

In today's digital age, data breaches and cyberattacks have become increasingly prevalent, threatening the confidentiality, integrity, and availability of sensitive information. Organizations in the healthcare industry often face even more risks—in fact, healthcare organizations have increasingly become the targets of ransomware and often have the highest costs associated with data breaches compared to other industries.

Healthcare organizations often have the highest costs associated with data breaches.

To combat these evolving threats and ensure the protection of valuable data, organizations in healthcare and across industries are adopting the HITRUST Common Security Framework (CSF), which has emerged as a leading approach to address security challenges effectively.

HITRUST was established in 2007 to address the unique security challenges faced by the healthcare industry. Since then, it has evolved into a comprehensive and flexible framework applicable to organizations beyond healthcare, becoming a benchmark for cybersecurity best practices. The HITRUST CSF combines multiple frameworks and standards, streamlining compliance requirements and reducing the burden on organizations. Let’s explore the 19 HITRUST domains that comprise the CSF, understanding their significance and how they contribute to overall information security.

Let's explore each of the 19 HITRUST domains.

HITRUST Domains 1 - 5

1. Information Protection Program

The Information Protection Program domain sets the foundation for the HITRUST CSF, focusing on the establishment of policies, procedures, and standards for safeguarding sensitive information. It includes elements such as establishing methodologies for risk assessments, incident response planning, and data classification, helping organizations identify vulnerabilities and prioritize risk mitigation efforts.

2. Endpoint Protection

This domain is concerned with securing endpoints like desktops, laptops, mobile devices, and servers, which are often vulnerable entry points for cyber threats. It encompasses robust security measures like intrusion detection systems, patches, firewalls, and software updates.

3. Portable Media Security

As the use of portable media devices increases, so does the risk of data loss and theft. This domain addresses the security challenges associated with the use of portable media, such as USB drives and external hard drives, by enforcing encryption and access controls to prevent unauthorized access to sensitive data.

4. Mobile Device Security

With the rising trend of remote work and the widespread use of mobile devices, securing these endpoints is critical. This domain focuses on implementing secure mobile device management policies, ensuring secure data transmission, and safeguarding remote work environments.

5. Wireless Security

As wireless technology becomes ubiquitous, it opens up potential vulnerabilities in an organization's network. The Wireless Security domain emphasizes the implementation of strong encryption, access controls, and monitoring mechanisms to protect against unauthorized access and data interception.

HITRUST Domains 6 - 10

6. Configuration Management

Effective configuration management is vital for maintaining the integrity and security of an organization's IT assets. This domain encourages organizations to establish configuration baselines, enforce change management policies, and regularly audit configurations to minimize vulnerabilities.

7. Vulnerability Management

Cyber threats continuously evolve, making vulnerability management a crucial aspect of any information security program. This domain focuses on identifying, assessing, and remediating vulnerabilities in software and systems to reduce the risk of exploitation.

8. Network Protection

Securing the network infrastructure is fundamental in preventing unauthorized access and data breaches. The Network Protection domain encompasses firewall management, network segmentation, and intrusion detection systems to fortify an organization's network perimeter.

9. Transmission Protection

The Transmission Protection domain concentrates on securing data during transmission between systems. Implementing encryption protocols and secure communication channels ensures that sensitive information remains confidential and unaltered while in transit.

10. Password Management

Passwords are often the first line of defense against unauthorized access. This domain promotes best practices in password management, such as strong password policies, multi-factor authentication (MFA), and regular password updates, reducing the risk of unauthorized access.

Did you know?

Healthcare breaches have been the most expensive industry breaches for over a decade.

HITRUST Domains 11 - 15

11. Access Control

Controlling access to sensitive data and systems is paramount in maintaining data confidentiality and preventing internal breaches. The Access Control domain emphasizes the principle of least privilege, ensuring that users only have access to the resources necessary for their roles.

12. Audit Logging and Monitoring

Comprehensive audit logging and monitoring are essential for detecting and responding to security incidents promptly. This domain stresses the implementation of robust logging mechanisms and real-time monitoring to identify suspicious activities and potential security breaches.

13. Education, Training, and Awareness

Human error remains a significant factor in security breaches. This domain underscores the importance of educating and training employees on cybersecurity best practices to create a security-conscious culture within the organization.

Educating and training employees on best cybersecurity practices can create a culture of security and compliance.

14. Third-Party Assurance

Organizations often collaborate with third-party vendors, increasing the need for third-party assurance. This domain focuses on assessing and managing the security risks associated with external partners, ensuring that they adhere to similar security standards.

15. Incident Management

Despite preventive measures, security incidents may still occur. The Incident Management domain outlines procedures for identifying, containing, and mitigating the impact of security incidents swiftly and effectively.

HITRUST Domains 16 - 19

16. Business Continuity and Disaster Recovery

In the face of unforeseen events, maintaining business continuity is essential. This domain emphasizes the creation of comprehensive business continuity and disaster recovery plans, ensuring that critical functions can resume in a timely manner.

17. Risk Management

The Risk Management domain is an essential part of the HITRUST CSF, as it requires organizations to conduct risk assessments and implement appropriate controls based on their risk posture. This iterative process helps organizations continuously improve their security posture.

18. Physical Environment and Safety

Even in today's digital age, organizations often have physical storage locations. This control domain is intended to help organizations handle the security requirements for physical storage locations of sensitive data.

19. Data Protection and Privacy

The purpose of this final control domain is to help organizations comply with privacy regulations. Given strict privacy laws like HIPAA, this domain is essential for organizations that want to avoid hefty fines.

Data breaches and cyber threats will continue to challenge organizations across industries. Embracing a robust and threat adaptive framework like the HITRUST CSF can significantly enhance an organization's ability to manage information security risks effectively. The 19 HITRUST domains provide a comprehensive and flexible approach to safeguarding sensitive data, fortifying network infrastructure, and fostering a culture of cybersecurity awareness. By adopting and implementing the HITRUST CSF, organizations can demonstrate their commitment to protecting their customers' data and building trust in an increasingly interconnected world.

About BARR Advisory

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Cybersecurity Consulting and vCISO Services**
- **Compliance Program Assistance**

Connect with BARR

Want to learn more about the HITRUST domains and how HITRUST compliance can benefit your organization?

Contact us today, or join us for an Open House every Wednesday from 11 a.m. to noon CST for a Q&A and discussion of the process and benefits of obtaining HITRUST certification.