

HITRUST®

Using a Controls Framework to Address NIST, HIPAA, and GDPR Security Requirements and to Ensure Management of Cyber Threats

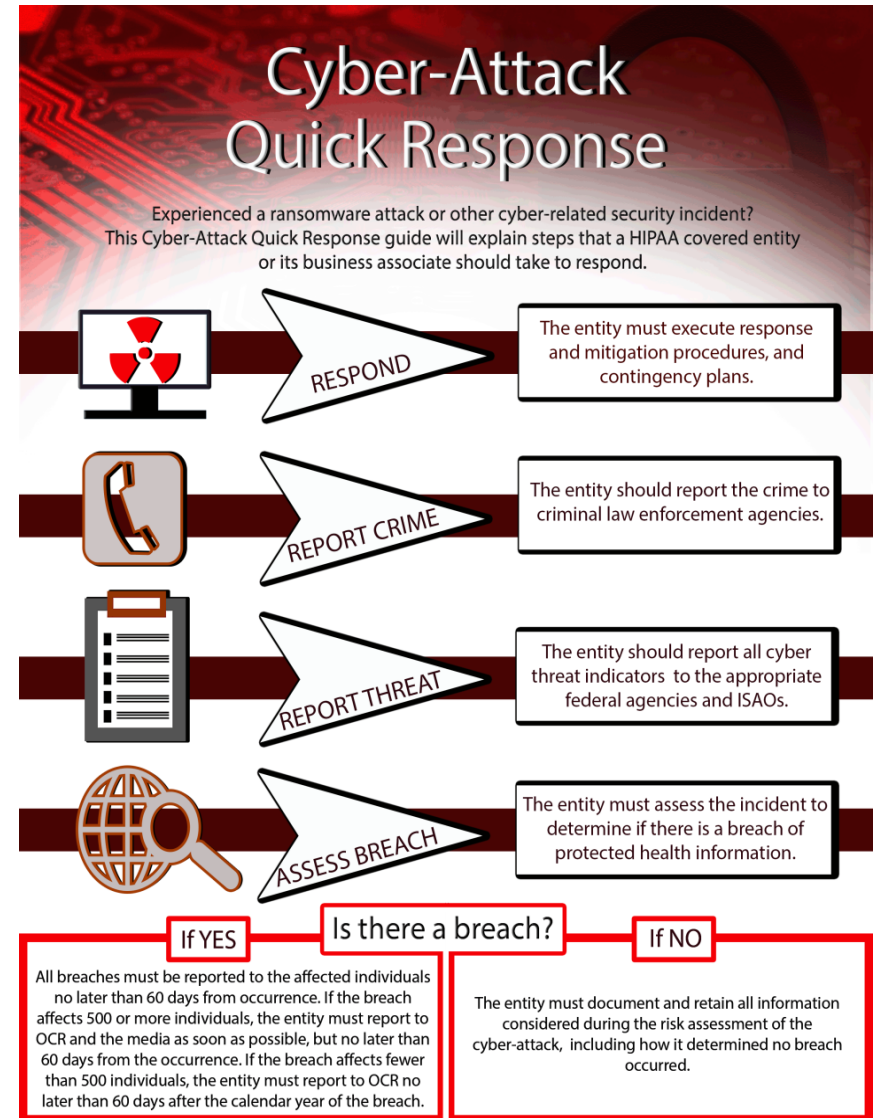
HITRUST



LEADING CYBER THREATS AND REGULATORY RESPONSE

Ransomware Attacks

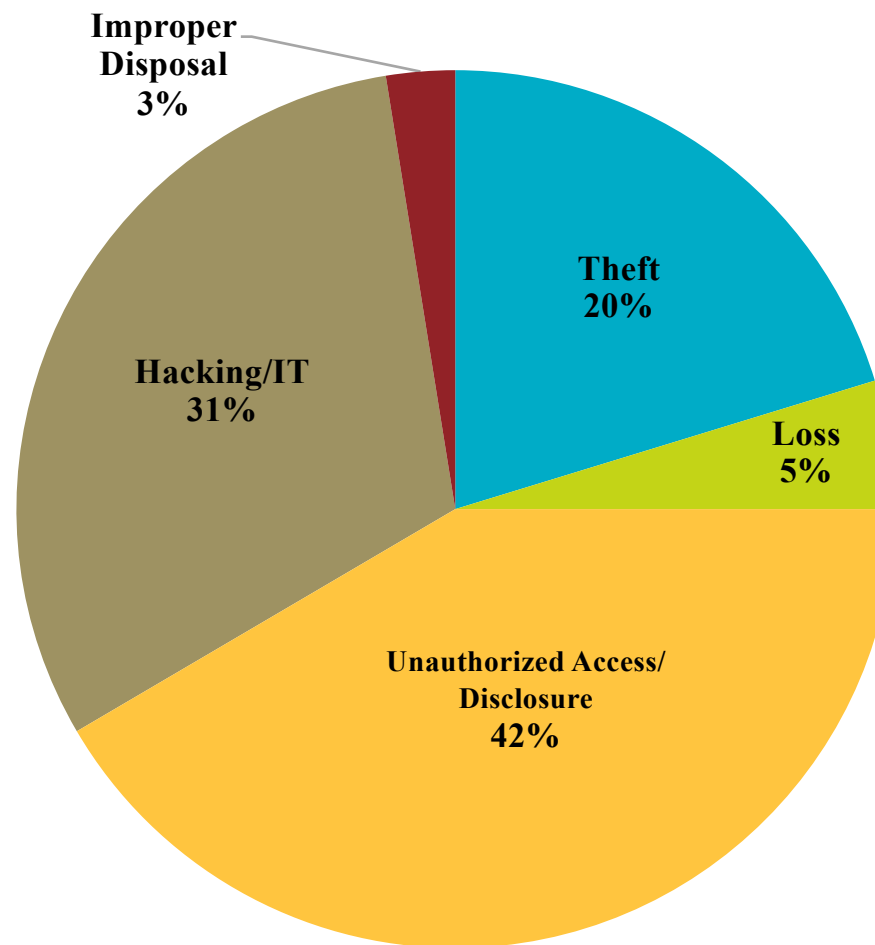
- Phishing and Ransomware
 - Security Awareness and Training and Security Reminders
 - Be Prepared
 - Practice!



HIPAA Breach Highlights

500+ Breaches by Type of Breach

9/1/2015 – 8/31/2018



Vendor Cyber Risk Management

- FTC Guidance: <https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series>
- NIST Guidance: <https://www.nist.gov/cyberframework>
- HHS Cloud Guidance: <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>
- HHS Business Associate Guidance: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es>
- Remote Access Issues

Insider Threat

- Organizations must “[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information ... and to prevent those workforce members who do not have access ... from obtaining access to electronic protected health information,” as part of its Workforce Security plan. See 45 C.F.R. § 164.308(a)(3).
- Appropriate workforce screening procedures could be included as part of an organization’s Workforce Clearance process (e.g., background and OIG LEIE checks). See 45 C.F.R. § 164.308(a)(3)(ii)(B).
- Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization’s workforce exit or separation process. See 45 C.F.R. § 164.308(a)(3)(ii)(C).
- February 16, 2017: Memorial Healthcare System (MHS)
 - \$5.5 Million
 - <https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html>

Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. See 45 C.F.R. § 164.312(e)(2)(ii).
- Applications for which encryption should be considered when transmitting ePHI may include:
 - Email
 - Texting
 - Application sessions
 - File transmissions (e.g., ftp)
 - Remote backups
 - Remote access and support sessions (e.g., VPN)
- June 10, 2015: St. Elizabeth's Medical Center (SEMC)
 - \$218,400
 - <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/semc/index.html>

Software Patching

- The use of unpatched or unsupported software on systems which access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.
- In addition to operating systems, EMR/PM systems, and office productivity software, software which should be monitored for patches and vendor end-of-life for support include:
 - Router and firewall firmware
 - Anti-virus and anti-malware software
 - Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

Training

- Most settlements include a training requirement
 - <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>
- OCR Publishes a Monthly Cybersecurity Newsletter
 - <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html>
- OCR YouTube Page
 - <https://www.youtube.com/user/USGovHHSOCR>

Recent HHS Security Enforcement Actions

- December 18, 2017: 21st Century Oncology
 - \$2,300,000
 - \$2.3 Million Levied for Multiple HIPAA Violations at NY-Based Provider
- February 1, 2018: Fresenius Medical Care North America (FMCNA)
 - \$3,500,000
 - Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules
- June 18, 2018: MD Anderson
 - \$4.3 Million CMP
 - Judge rules in favor of OCR and requires a Texas cancer center to pay \$4.3 million in penalties for HIPAA violations
- October 15, 2018: Anthem
 - \$16 Million
 - Anthem Pays OCR \$16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History

Recent FTC Security Enforcement Actions

- Nov 29, 2017:
 - FTC Gives Final Approval to Settlements with Companies that Falsely Claimed Participation in Privacy Shield
- Nov 8, 2017:
 - FTC Gives Final Approval to Settlement with Online Tax Preparation Service
- Aug 15, 2017:
 - Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims
 - Final Approval October 26, 2018: https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber?utm_source=govdelivery
- Feb 27, 2018:
 - PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act
- June 6, 2018
 - U.S. Court of Appeals, 11th Circuit Ruling in LabMD, Inc.
 - <http://media.ca11.uscourts.gov/opinions/pub/files/201616270.pdf>

The background of the slide is a detailed, high-resolution image of a red printed circuit board (PCB). The board is covered in a complex network of fine, winding lines representing electrical traces. Numerous circular pads and larger, irregular shapes representing component footprints are visible throughout the design. The overall color is a deep, vibrant red, giving it a technological and secure appearance.

CYBERSECURITY REQUIREMENTS/CONTROLS

GDPR Requirements

- In the European Union's General Data Protection Regulation (GDPR), Article 32 requires, "Appropriate technical and organizational measures to ensure a level of security appropriate to the risk"
- Examples include:
 - Encryption
 - Pseudonymization
 - Business Continuity/Disaster Recovery
 - "Regularly testing, assessing and evaluating the effectiveness of technical and organisational measures"
 - Evaluating processors/contractors

Other International Standards

- Canada, Singapore, China, and many other countries have similar language in their laws as do data sharing frameworks internationally about “adequate” security
- Too vague to be implemented on its own

HIPAA Security Rule

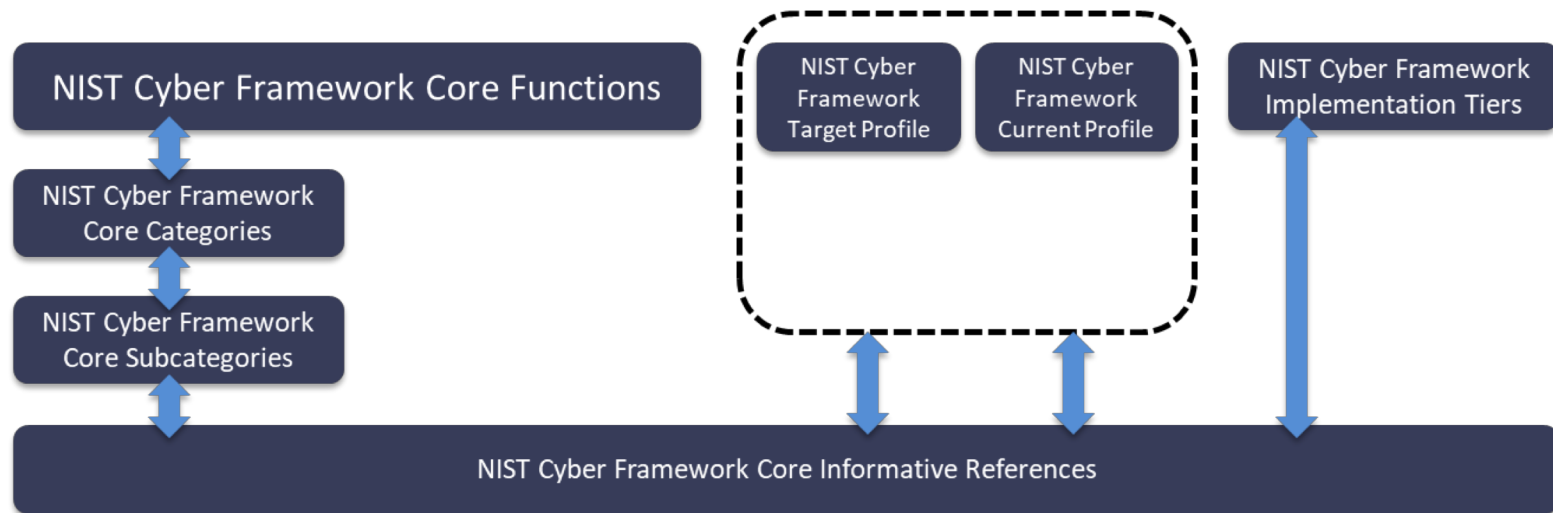
- The HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) details the security requirements for HIPAA covered entities and business associates
- A risk analysis and appropriate response thereto is key to HIPAA security compliance
- Based on a review of the requirements from the Rule and the results of a risk analysis, an entity can identify gaps in its security posture and implement corrective action plans
- The risk analysis can also serve as the basis for decision making regarding addressable requirements in the Security Rule

The background of the slide is a dark red color with a complex, glowing circuit board pattern. The circuitry consists of numerous interconnected lines, loops, and circular nodes, resembling a printed circuit board (PCB) or a microchip layout. The lines vary in thickness and form, creating a dense, technical aesthetic. The overall effect is one of high-tech and digital security.

Implementing the NIST Cybersecurity Framework and Addressing
Regulatory Requirements for the Protection of Personal Data

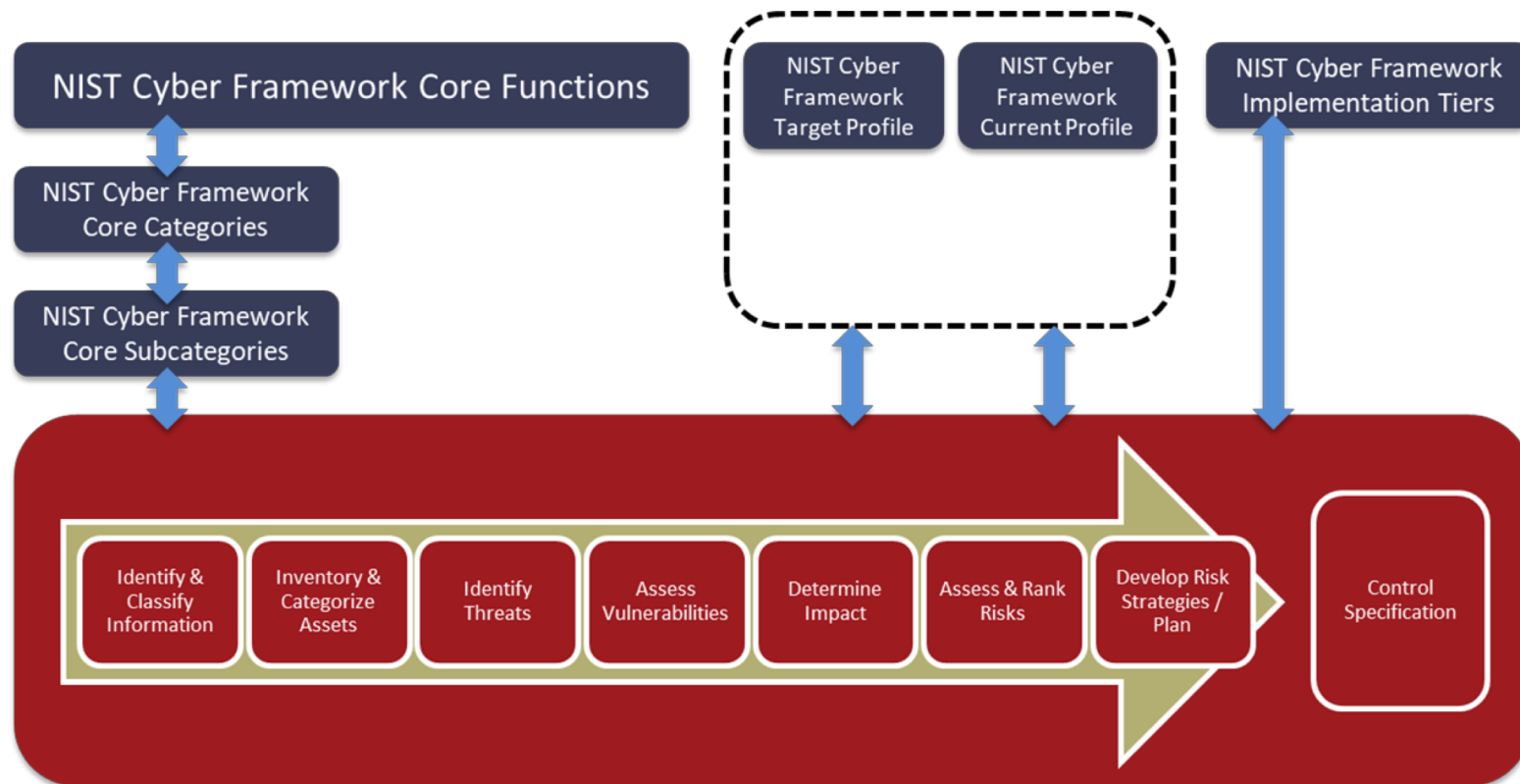
FRAMEWORK-BASED RISK ANALYSIS AND CONTROL SPECIFICATION

The NIST Cybersecurity Framework



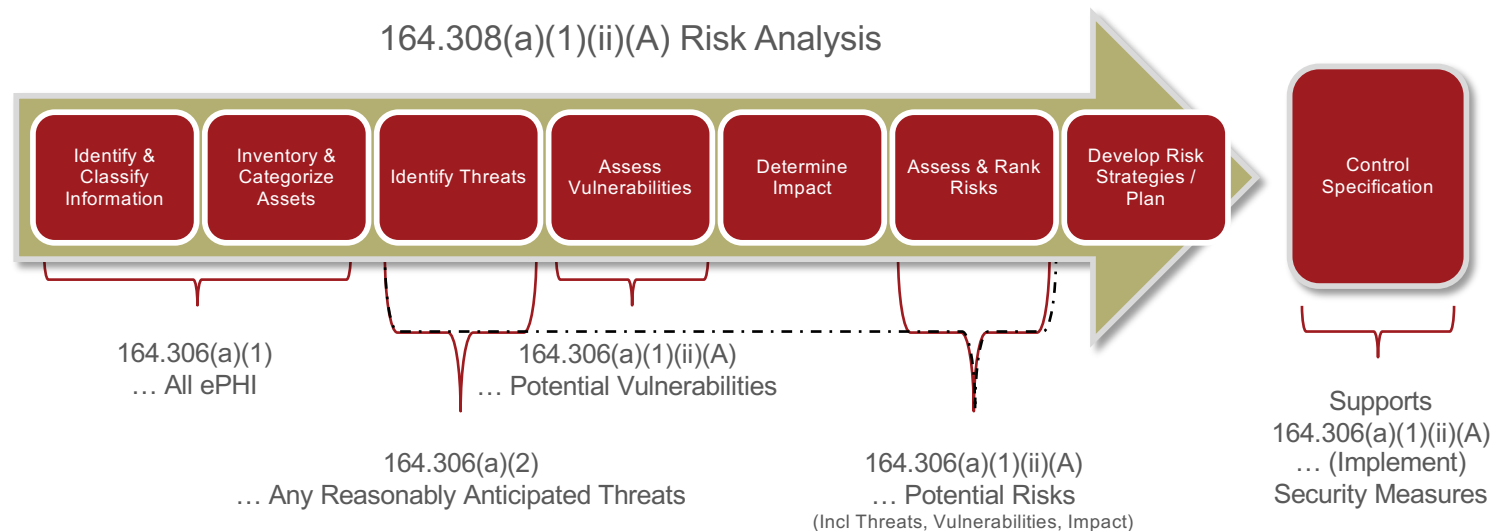
- Provides an overarching set of guidelines intended to provide consistency as well as depth, breadth and rigor of organizational cybersecurity programs
- Complements rather than replaces an organization's existing business or cybersecurity risk management process and cybersecurity program
 - Simply because the NIST Cybersecurity Framework lacks the prescription necessary for an organization to implement a program that achieves the many and varied outcomes specified by the Core Subcategories ... hence the Informative References

Risk Analysis & Control Specification



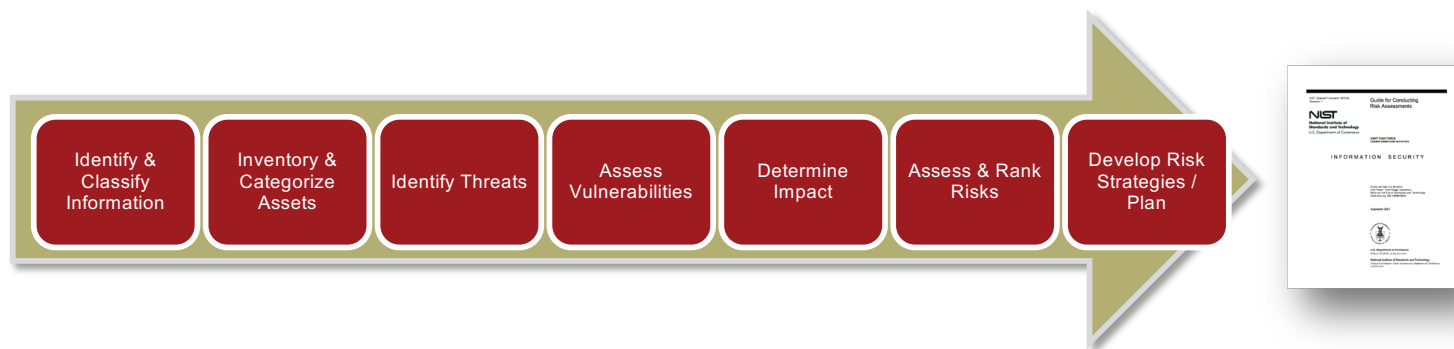
- Informative References provide an incomplete specification of necessary controls
- Do not necessarily address regulatory or due care and due diligence obligations

Risk Analysis According to HIPAA



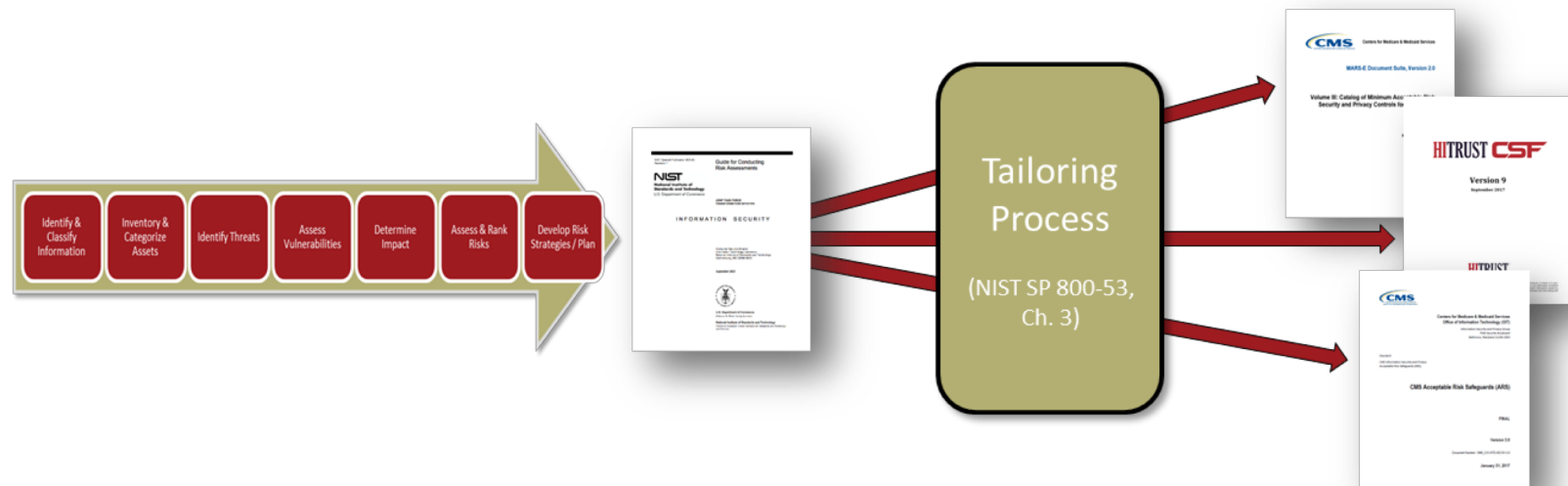
- The end result of risk analysis is a control specification that is intended to mitigate the risk associated with all “reasonably anticipated threats” to the security of ePHI
- Unfortunately, as is indicated by two rounds of OCR audits, traditional risk analysis is difficult, especially for smaller healthcare providers
- *If only there was another way we could leverage the NIST Cyber Framework’s Core Illustrative References ...*

NIST Risk Management Framework (RMF)



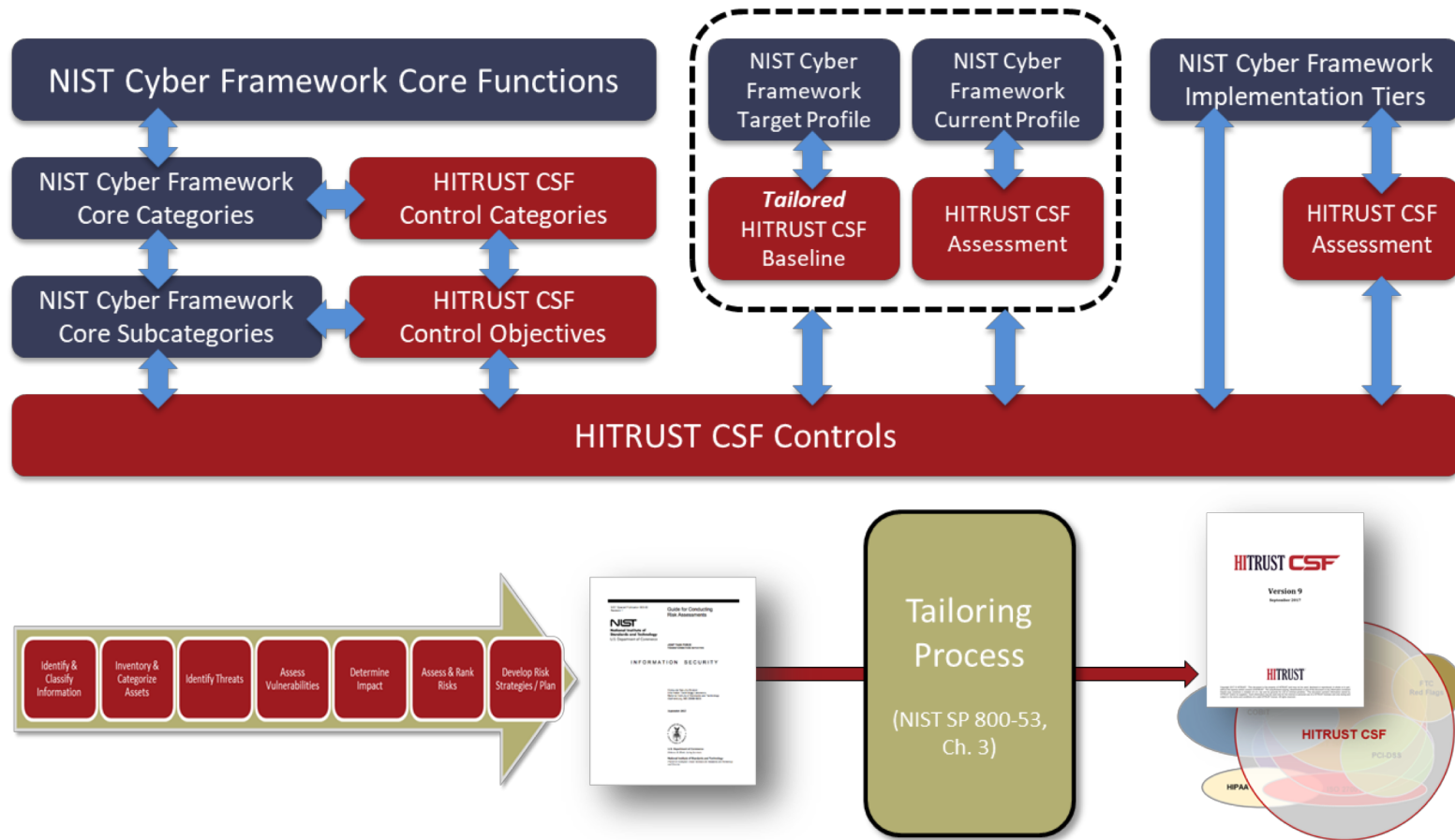
- NIST RMF embodied in multiple FIPS & NIST SP 800-series publications
- Primary documents are FIPS 199 (categorization) & NIST SP 800-53 (controls)
- Risk analysis is of common threats to sensitive information the federal government uses, a set of vulnerabilities common to the types of technology, systems, and information architectures generally used by the federal government, and categorization of the impact due to a loss of information security
- An appropriate baseline is selected based on level of impact—low, moderate or high—which federal agencies select to complete the risk analysis
- Agencies are then expected to tailor the NIST baseline to their specific needs

Healthcare Overlays of NIST SP 800-53



- An overlay* is a fully specified set of security controls, enhancements and supplemental guidance derived through the tailoring process
- Overlays help organizations achieve standardized security capabilities, consistency of implementation, & cost-effective security solutions, & may support
 - Industry/sectors (e.g., healthcare, public health)
 - Information technology (e.g., medical devices, cloud services)
 - Coalitions/partnerships (e.g., Joint HITRUST™ certification & EHNAC accreditation)
 - Statutory/regulatory requirements (e.g., HIPAA, PCI)
- Overlays become the new “gold standard” for the intended “community-of-interest”

Leveraging the HITRUST Overlay



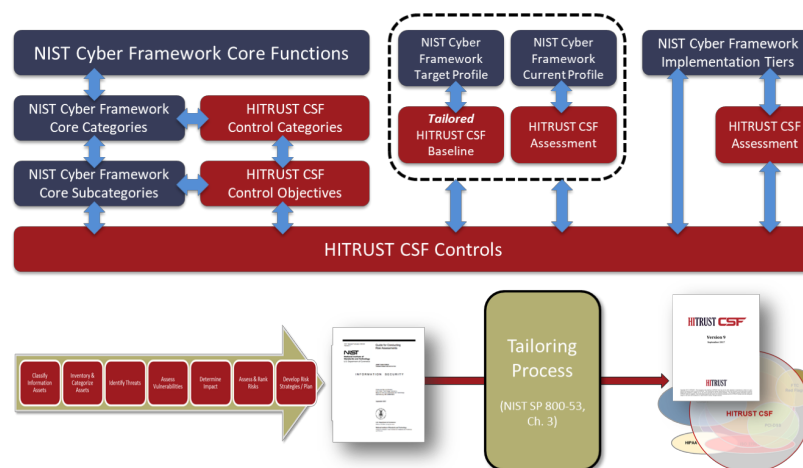
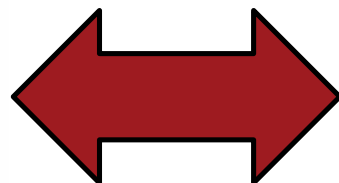
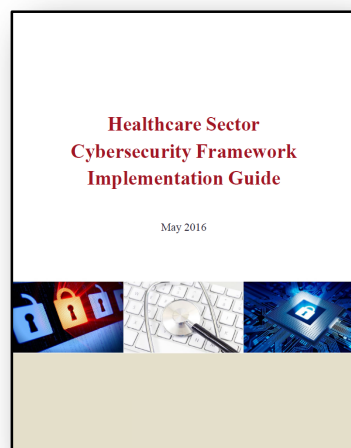
Comparison of Risk Analysis Approaches

Traditional Risk Analysis	Framework-based Risk Analysis
<ul style="list-style-type: none"> • Must be applied to all assets where ePHI “lives” 	<ul style="list-style-type: none"> • Must be applied to all assets where ePHI “lives”
<ul style="list-style-type: none"> • <i>Must ensure a complete evaluation of anticipated threats & known vulnerabilities (i.e., starting at 0%) to design a comprehensive set of information security controls</i> 	<ul style="list-style-type: none"> • <i>Although significant tailoring is done to create the overlay (starting at 80%*), the organization <u>must</u> perform additional tailoring via a targeted risk analysis to address any unique threats & vulnerabilities (for the additional 20%*)</i>
<ul style="list-style-type: none"> • Must be applied intelligently to specific assets within the organization 	<ul style="list-style-type: none"> • Must be applied intelligently to specific assets within the organization

* Analogous to the Pareto Principle (also known as the 80/20 Rule, the law of the vital few, or the principle of factor sparsity), which states that, for many events, roughly 80% of the results (effects) come from 20% of the effort (causes). In this case, an organization must only provide a limited amount of effort to obtain a near complete specification of the security controls required to address reasonably anticipated threats to the sensitive information it uses.

HPH Sector Guidance on NIST Cyber Framework Implementation

Guidance on implementing the NIST Cyber Framework leveraging the HITRUST RMF was developed through the Healthcare and Public Health (HPH) Government and Sector Coordinating Councils (GCC/SCC), which is a public-private partnership that includes DHS, HHS and numerous industry organizations and associations




Available from the DHS US-CERT Cybersecurity Framework Website at
https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

The background of the slide is a detailed, high-resolution image of a red printed circuit board (PCB). The board is covered in a complex network of fine, winding copper traces and numerous circular solder pads. Several larger, rectangular components, possibly integrated circuits or connectors, are visible, some with multiple pins or connection points. The overall color scheme is a deep, vibrant red, giving it a technological and industrial feel.

INCENTIVIZING USE OF CONTROLS FRAMEWORKS

Incentivizing Use of Controls Frameworks

- Company resources are limited, and while the C-suite is increasingly sensitive to privacy and security concerns, there are still issues getting sufficient resources to the necessary departments
- While there is much research on the return on investment for privacy and security programs, a more solid foundation of recognition of the use of assurance programs based on controls frameworks would add clear ROI.
- We are already seeing companies requiring such assurance programs be used by third party vendors to control supply chain risk.
- Governmental recognition of these programs would increase their visibility at the C-suite level and provide additional incentives to adopt such programs
- Some clichés are true – a data sharing system is only as strong as its weakest link
- We need to encourage more privacy and security assurance program use to ensure the weakest link is not, in fact, weak



Polsinelli PC provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

© 2018 Polsinelli® is a registered trademark of Polsinelli PC. In California, Polsinelli LLP.



Polsinelli PC, Polsinelli LLP in California | polsinelli.com

Disclaimer

The descriptions contained in this communication are for preliminary informational purposes only and should not be taken as legal advice. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd's. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497). CBEM665_US_09/18

HITRUST 2018 Snapshot

Background

1. Founded in 2007
2. HITRUST Alliance, Inc. is a non-profit responsible for frameworks, standards and methodologies
3. HITRUST Service Corporation is a for-profit responsible for training and tools



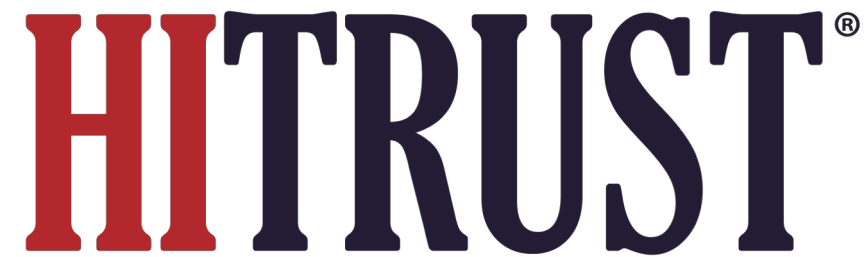
Best Known For

1. Developing the HITRUST CSF – 9th major release
 - Development guided by a CSF Advisory Council comprised of AHA, AMA, AHIP, AGMA and other security/privacy experts
 - Basis for the health and public sector implementation guidance for the NIST Cybersecurity framework, recognized by Department of Homeland Security ([link](#)) and Department of Health and Human Services ([link](#))
 - Deemed an acceptable controls criteria by the AICPA for a SOC 2 examination
 - Identified as an appropriate standard to safeguard Internet of Things (IoT) by NIST ([link](#))
2. Operating the healthcare industry's Information Sharing and Analysis Organization (ISAO)

Adoption

1. HITRUST CSF is utilized by 81% of US hospitals and health systems and 83% of US health plans
2. HITRUST CSF is the most widely adopted control framework in the healthcare industry, according to a 2018 HIMSS survey
3. HITRUST CSF Assurance program is the most widely adopted program for assessing third party risk





Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the [Content Spotlight](#)