Introduction to the HITRUST CSF Threat Catalogue™

Supporting risk analysis and the consumption of threat intelligence

v. HT-401-02

www.HITRUSTAlliance.net

HITRUST®

Executive Summary

The HITRUST CSF® is updated at least annually based on relevant new or updated authoritative sources, such as regulations, standards, and best practices, as well as due to changes in technology or root causes of data losses and breaches. Even so, the HITRUST CSF may not be as responsive to a changing threat environment as one would like, as the frequency of updates to the underlying authoritative sources can range from years—as with NIST SP 800-53—to almost a decade—as with ISO/IEC 27001. Subsequently, any organization relying on the next release of any control framework, not just the HITRUST CSF, will always be slightly more reactive than an organization that has the capability to conduct the ongoing analyses necessary to address unique, active, or emergent threats.

Identifying threats is a major component of a comprehensive risk analysis process for any organization seeking to protect their sensitive data and helps determine what adverse events are relevant to the organization and must be controlled. For example, the increased frequency of ransomware attacks required organizations—of all types and sizes—to re-examine their controls around data backup and restoration and ensure they could successfully recover their data if such an attack occurred.

HITRUST® 'stands on the shoulders of giants' and relies on the risk analyses performed by authors of the underlying control frameworks and other authoritative sources integrated into the HITRUST CSF. However, understanding how the HITRUST CSF controls address extant and emerging threats would not only help HITRUST make the framework more responsive, but it would also allow organizations leveraging the framework to be more responsive as well.

Unfortunately, a comprehensive threat list that could support risk analysis and help organizations better understand and mitigate threats to sensitive information was generally unavailable, so—given the significance—HITRUST set out to identify a complete set of threats at a level consistent with the HITRUST CSF control requirements used to address them.

The result is the HITRUST Threat Catalogue™, which consists of a PDF file listing what is intended to be a mutually exclusive and collectively exhaustive enumeration of threats, and an XLS file that provides a mapping of these threats to specific technical, physical, and administrative controls in the HITRUST CSF v9.4.x along with associated definitions.

Threats have been categorized in what is thought to be a logical grouping of types, categories, and sub-categories. The Threat Catalogue has three types of threats which are logical, physical, and organizational. Each type of threat will have categories such as intentional, unintentional, and force majeure. Sub-categories further refine the categories into specific descriptors of the threat activity. Each threat has a unique identifier consisting of the first character from the name of each hierarchical level combined with a numerical value; for example: logical, intentional, and conflict resulting in 'LIC,' and threats listed as 0, 1, and so on.

Users of the Threat Catalogue are cautioned in that—as with any tool—it has certain limitations. For example, the Threat Catalogue is not intended to address threats that do not impact the confidentiality, integrity, or availability of sensitive information, nor is it intended to provide a list that is more granular than the control requirements in the HITRUST CSF. It also does not support threat modeling for specific applications or architectures, although it could be leveraged in the general threat modeling process.

Questions We’ll Address

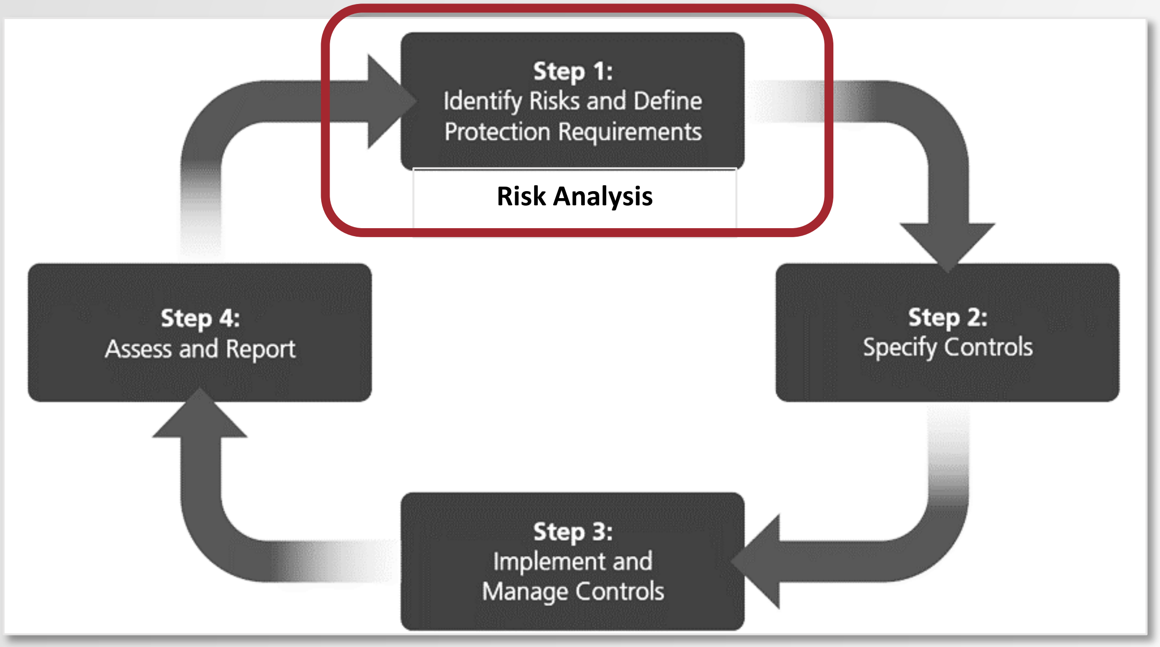
1. Why do we need a threat catalogue?
2. What exactly is a threat catalogue?
3. What is the HITRUST Threat Catalogue?
4. What are the goals and benefits?
5. How does it relate to the HITRUST Approach?
6. How will it continue to evolve and improve?
7. What other questions are frequently asked?

Section 1

WHY DO WE NEED A THREAT CATALOGUE?

Risk Management and Analysis

- *Risk* is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the probable adverse impact should the circumstance or event occur and the likelihood of its occurrence.
- *Risk Management* consists of the program and supporting processes to manage information security risk to the organization.
- *Risk Analysis*, the first step in the risk management process, is an examination of information to identify the risk to an information asset. Synonymous with risk assessment.


Step 1:
Identify Risks and Define Protection Requirements
Risk Analysis
Step 2:
Specify Controls
Step 3:
Implement and Manage Controls
Step 4:
Assess and Report

Security risk is essentially an event that may happen and potentially have a bad result. Basically, “stuff happens.” But, while security risk is often viewed as only negative, risk may be both positive and negative. Gambling is a perfect example of this.

Risk management is essentially all the things we do to manage our risk to something we find comfortable. For example, we may limit ourselves to $100 per night while gambling in Vegas, and we don’t gamble any of our winnings (if we’re lucky) from any prior night of gambling.

Risk analysis is what we do to determine what risks we need to control. For example, we may look at the expected payoffs and our relative skills for various forms of gambling we like, such as Roulette and Craps. We may also recognize that drinking while gambling results in degraded judgement. And, of course, will gambling adversely impact the family budget?

Home security provides another example:

> ***Step 1:*** How much protection do we need? Are we in a safe neighborhood? One that has a high crime rate? Do we have a lot of valuables in the home?
>
> ***Step 2****:* How will we protect your home? Standard or high-security doors and locks? Bars on the windows? Do we need an alarm system? Do we need a monitoring service?
>
> ***Step 3:*** We need to install the doors, locks, bars, and alarms.
>
> ***Step 4:*** We need to make sure these protections continue to operate effectively. Are our locks susceptible to opening by a bump key? Are the bars on the windows coming loose?
>
> And finally, we need to repeat the process from time to time. But we don’t need to start from scratch, only address what may have changed. Has the crime rate gone up, e.g., has there been a rash of burglaries in the neighborhood? Did we start a home business and now have more items and/or information to protect?

More on Risk Analysis

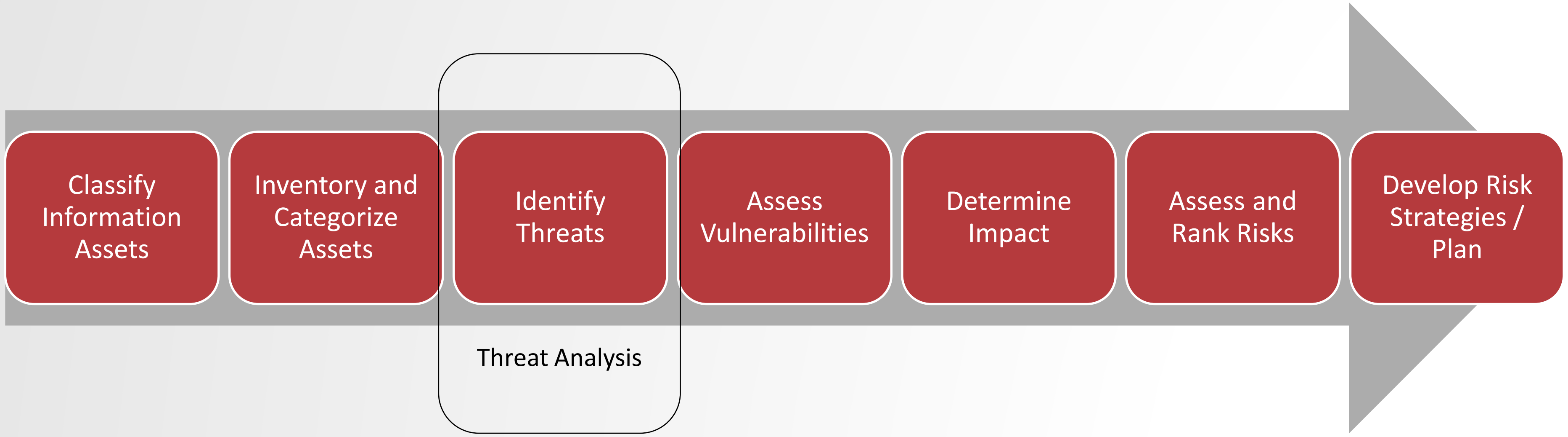
Risk assessment (synonymous with analysis, according to NIST and other government sources) is also a multi-step process, one view of which consists of seven steps: classification, inventory, threat analysis, vulnerability analysis, impact analysis, ranking risks, and developing a risk treatment strategy.

The end result of risk assessment is the information for the next step in the risk management process, which is the specification of the comprehensive set of reasonable and appropriate information security controls needed to adequately protect personal data and other sensitive information.

However, many organizations fail in conducting their risk analysis, and the reason is quite simple: Risk analysis is hard.

Some of the reasons for a failed analysis include, but are not limited to, an incomplete asset inventory, failure to categorize assets properly, limited or no understanding of asset value, *a failure to enumerate/address all reasonably anticipated threats*, inability to determine the likelihood of a threat occurrence or impact, control effectiveness interpreted as risk, no documentation of risk treatments (especially of risk acceptance), and the failure to address corrective actions for all risks requiring mitigation.

Of these, the *threat analysis* is perhaps one of the most difficult for many organizations due to a lack of information and, in many cases, a lack of expertise.

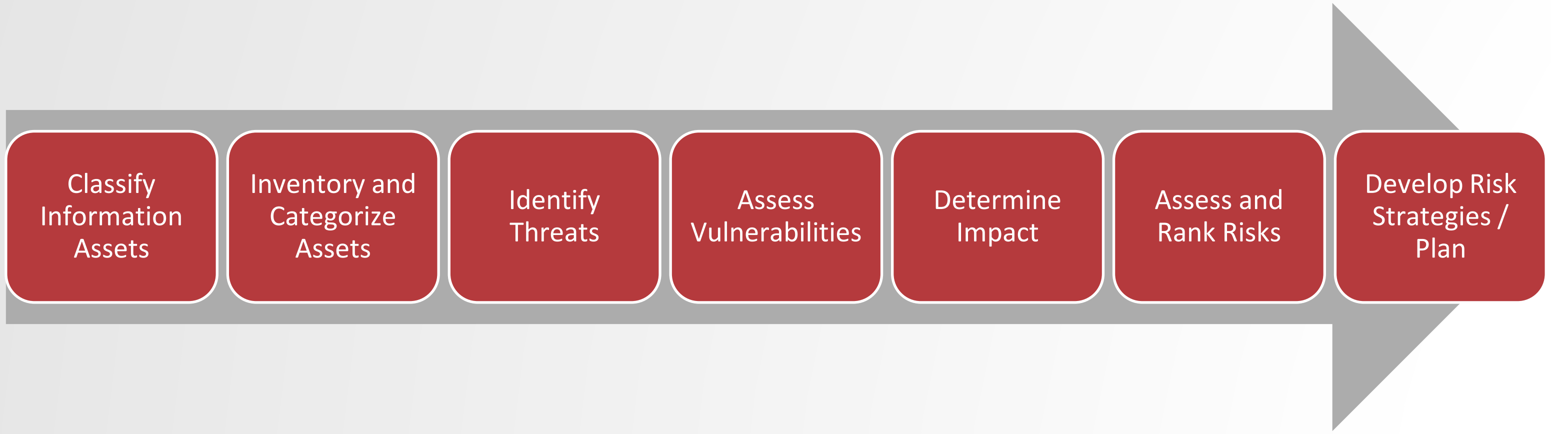


Control-based Risk Analysis

However, it is possible to complete the risk analysis without actually having to do one (at least from 'scratch'). Instead, organizations can rely on a comprehensive control framework, which is already built upon a broad analysis of threats faced by similar types of organizations using similar information technologies for processing information requiring similar levels of protection. This is the approach employed by the U.S. intelligence community, Department of Defense, and civilian agencies of the federal government with their respective information security control and risk management frameworks.

This framework is embodied in multiple NIST Special Publications and Federal Information Processing Standards, or FIPS publications, the core of which is FIPS Pub 199, which standardizes the way information and information systems are categorized, and NIST SP 800-53, which specifies minimum security control baselines—i.e., a minimally acceptable set of information security protections—that are determined based on how that information is categorized.

To do this, NIST conducted a risk analysis for three different types of information based on their relative sensitivity and level of criticality—basically, the importance of the information's confidentiality, accuracy, and availability to the organization. With respect to the three principal components of risk analysis, NIST identified a set of common threats to information that 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 broke out the impact due to a loss of information security into low, moderate, and high. NIST then specified a set of security controls considered to provide a minimally acceptable level of protection for each of these three types of information. Subsequently, all a federal organization needs to do to complete the NIST risk analysis is to determine the category of the information it wants to protect, which is a very easy thing to do—especially when compared to what's involved in the rest of the risk analysis.



Classify Information Assets

Inventory and Categorize Assets

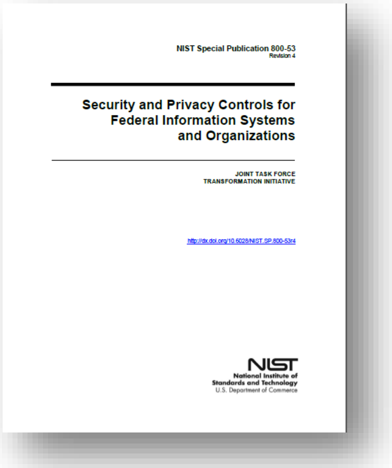
Identify Threats

Assess Vulnerabilities

Determine Impact

Assess and Rank Risks

Develop Risk Strategies / Plan



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for
Federal Information Systems
and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

HITRUST Overlay of the NIST Moderate-Impact Control Baseline

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, and cost-effective security solutions, and may support:

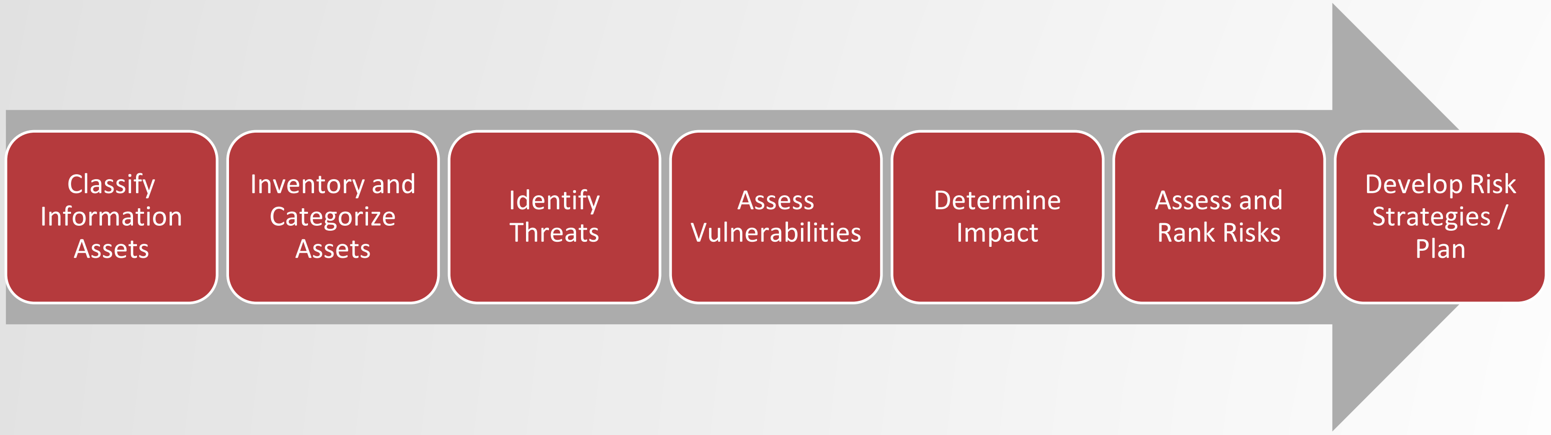
- Industry/sectors (e.g., healthcare, public health)
- Information technology (e.g., medical devices, cloud services)
- Coalitions/partnerships (e.g., joint HITRUST CSF Certification & EHNAC accreditation)
- Statutory/regulatory requirements (e.g., HIPAA, PCI)

Overlays become a new minimally acceptable security control baseline—the new “gold standard”—for the intended “community of interest.”

In fact, the Centers for Medicare and Medicaid Services (CMS) developed two sets of minimum-security control baselines to do just that:

- CMS Information Systems Acceptable Risk Safeguards
- Minimum Acceptable Risk Standards for Exchanges

It is this approach that HITRUST also used to create a security controls-based risk management framework that could provide a semi-custom yet consistent, comprehensive, and prescriptive set of security controls for both public and private sector organizations.



Classify Information Assets

Inventory and Categorize Assets

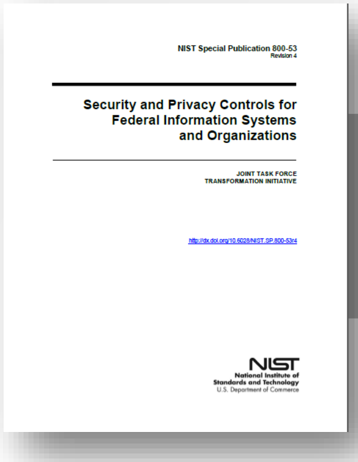
Identify Threats

Assess Vulnerabilities

Determine Impact

Assess and Rank Risks

Develop Risk Strategies / Plan



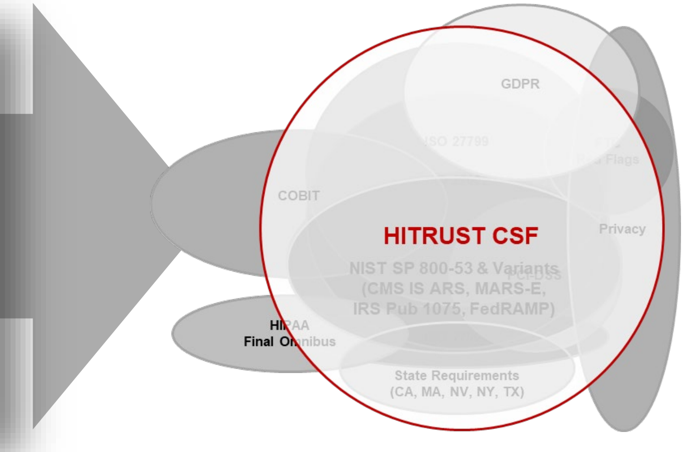
NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for
Federal Information Systems
and Organizations

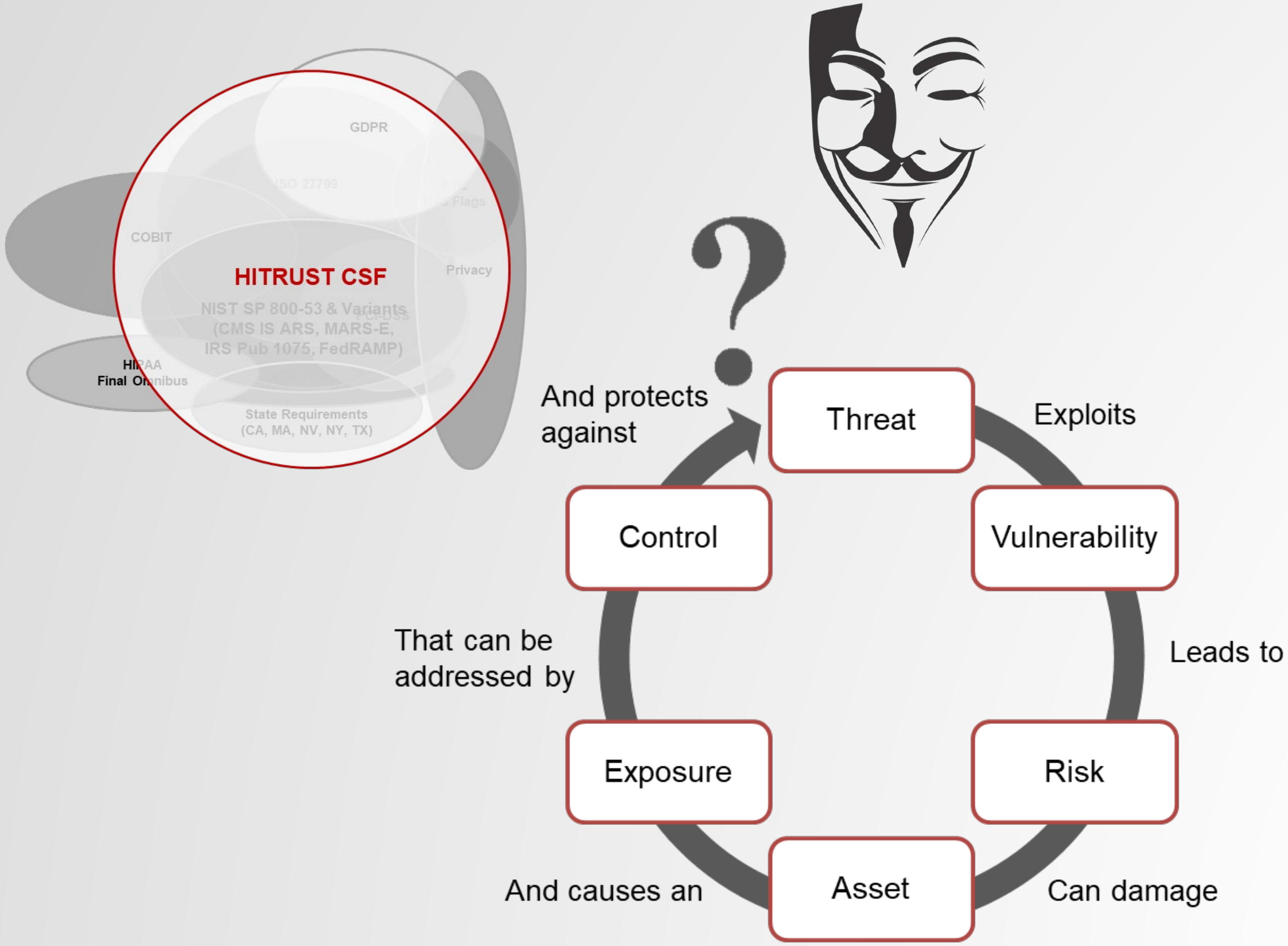
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



Why We Need a Threat Catalogue



Threat

Exploits

Vulnerability

Leads to

Risk

Can damage

Asset

And causes an

Exposure

That can be addressed by

Control

And protects against

It’s obvious that leveraging a control-based risk management framework, such as that provided by NIST SP 800-53 or the HITRUST CSF—which integrates multiple standards and best practice frameworks like NIST SP 800-53—obviates the need for a traditional risk analysis and greatly facilitates specification of a comprehensive and robust set of information security controls.

However, as shown above, controls are meant to address specific risks posed by specific threats to information assets. And since the threat environment is known to be extremely dynamic, an organization’s controls must be continually evaluated against these changing threats to ensure its information assets remain adequately protected.

Unfortunately, control frameworks are relatively static and, in many cases, aren’t updated for years at a time. And even though the HITRUST CSF is updated no less than annually, updates are generally tied to changes in its multiple authoritative sources (such as NIST SP 800-53) and an analysis of historical breach data.

While more responsive than other control frameworks, updates to the HITRUST CSF controls are not as forward-looking as one might achieve by performing a traditional risk analysis, which—if done properly—allows an organization to consider extant and emerging threats when updating its specified controls.

Section 2

WHAT EXACTLY IS A THREAT CATALOGUE?

Threat Catalogues

Definition

There is no generally accepted definition of the term “threat catalogue.” In practice, a threat catalogue can be as simple as a high-level threat taxonomy or as complicated as a completely enumerated threat list with a discussion of the controls that an organization could implement to address those threats.

INTERNATIONAL STANDARD
ISO/IEC 27005
Information technology — Security techniques — Information security risk management
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Guide for Conducting Risk Assessments
INFORMATION SECURITY
enisa
ENISA Threat Taxonomy
A tool for structuring threat information
INITIAL VERSION
1.0
JANUARY 2016
IT-Grundschutz-Catalogues
13th version - 2013
www.bsi.bund.de

Examples

Although somewhat inconsistent—if not disjointed—publicly available threat catalogues include, but are not limited to, the following:

- National Institute of Standards & Technology (NIST) SP 800-30: Provides approx. 100 threat events as part of its discussion of the NIST risk analysis process
- European Union Agency for Network and Information Security (ENISA) Threat Taxonomy: Provides a classification of threat types and 170 threats at various levels of detail
- International Organization for Standardization (ISO) 27005 *(available for a fee)*: Provides a list of less than four dozen threats
- Bundesamt fur Sicherheit in der Informatiionstechnik (BSI) IT-Grundschut-Katalog: Provides a comprehensive list of 370 threats along with a discussion and examples for each

Note: None of the available threat catalogues listed currently provide a mapping to ISO or NIST controls.

Section 3

WHAT IS THE HITRUST THREAT CATALOGUE?

The HITRUST Threat Catalogue Package

What it is …

The HITRUST Threat Catalogue provides a list of ‘reasonably anticipated’ threats, enumerated at a level commensurate with HITRUST CSF control requirements, and maps these threats to HITRUST CSF v9.4.x controls at a level commensurate with their specification (i.e., description of the control). Examples of the risk statements used to help determine an appropriate level of granularity for these threats are provided in the table below.

What it consists of …

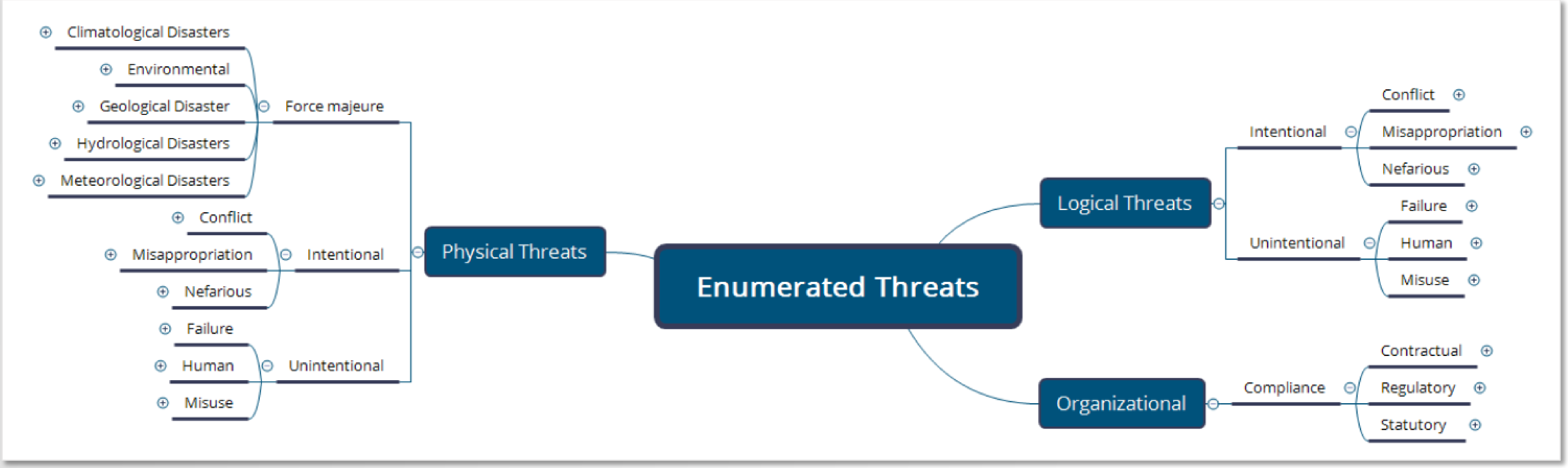
The HITRUST Threat Catalogue consists of four documents:

- **Introduction to the HITRUST Threat Catalogue** (this document)
- **HITRUST Enumerated Threat List**
- **HITRUST Threat Catalogue**

A threat source	*Performs a threat*	By exploiting a vulnerability	Introducing a risk	Which requires a control
A workforce member	*Steals equipment* *(Theft)*	By entering a nonsecure storage area	Resulting in a loss of availability	Which requires equipment to be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access *(Control 08.g, Specification)*
The organization	*Damages equipment* *(Accidental Damage)*	By not controlling humidity in storage areas	Resulting in a loss of availability	Which requires the installation of dehumidification equipment in storage areas (*Control 08.j, Requirement*)
The organization	*Incurs excessive down-time* *(Accidental Damage)*	Because of poor maintenance	Resulting in a loss of availability	Which requires the organization to maintain equipment correctly to ensure its availability and integrity (*Control 08.g, Specification*)
Third parties	*Obtain unauthorized access* *(Data Remanence)*	When performing depot-level maintenance	Resulting in a loss of confidentiality	Which requires local maintenance personnel to clear sensitive information from equipment before shipping it off for depot-level maintenance (*Control 08.j, Requirement*)
A system administrator	*Erases logs* *(Abuse of Authorizations)*	Because of his/her elevated privileges	Resulting in a loss of accountability	Which requires the protection of logging facilities and log information against tampering and unauthorized access (*Control 09.ac, Specification)*
The organization	*Loses log data* *(Storage Failure)*	Due to a lack of capacity planning	Resulting in a loss of accountability	Which requires the organization to securely archive logs before operational capacity is exceeded (*Control 09.ac, Requirement*)

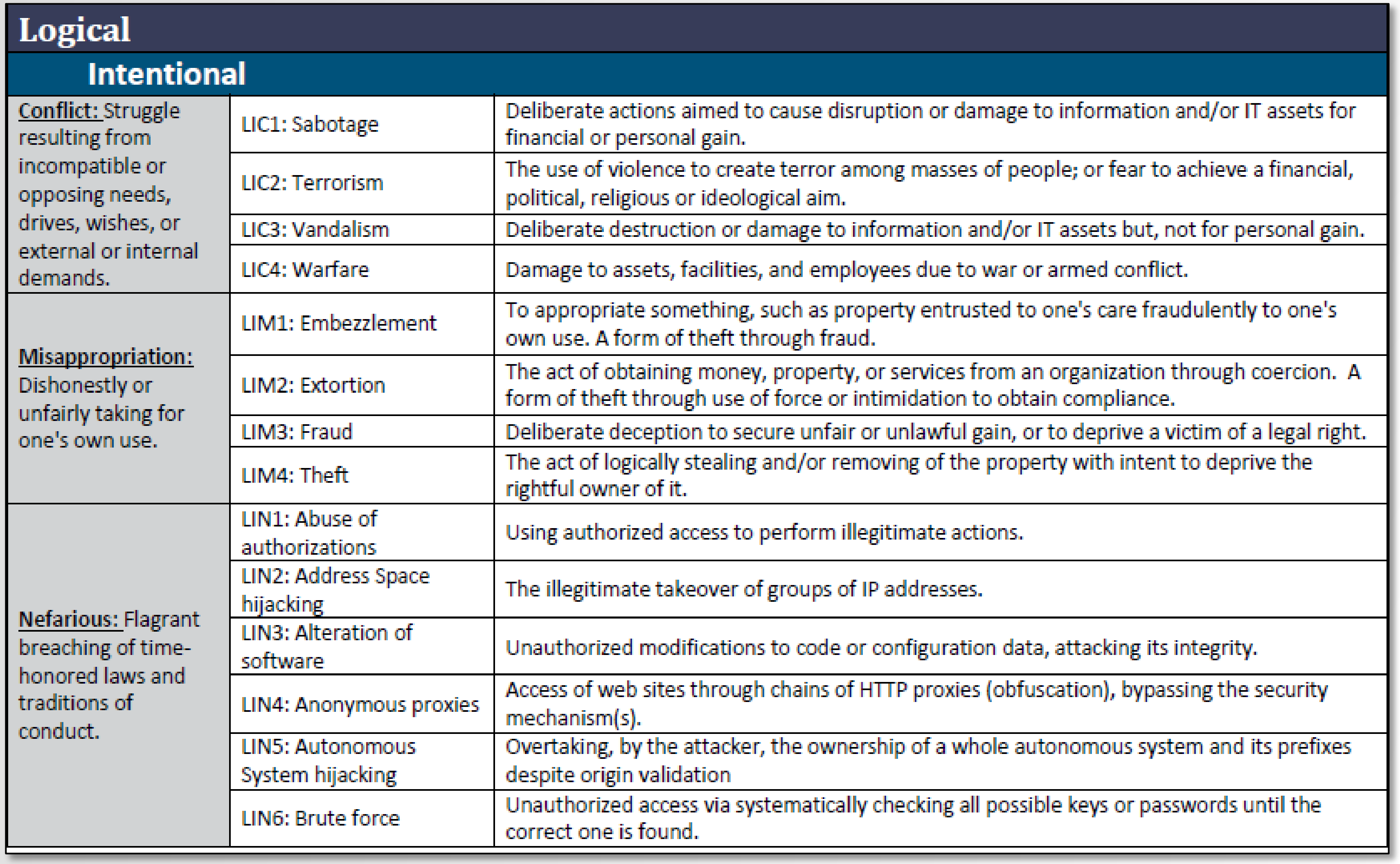
HITRUST Enumerated Threat List (1)

The *HITRUST Enumerated Threat List* proposes a four-level threat taxonomy consisting of threats, threat sub-categories, threat categories, and threat types. The intent is to provide a classification schema—shown below—that supports a mutually exclusive and collectively exhaustive enumeration of threats to sensitive information, such as personal data, that is specified at a level commensurate with the level of granularity found in the HITRUST CSF control requirements. The document also provides a detailed list of 'reasonably anticipated' threats as well as a set of definitions the reader may find helpful.



HITRUST Enumerated Threat List (2)

Enumerated Threats



Logical		
Intentional		
Conflict: Struggle resulting from incompatible or opposing needs, drives, wishes, or external or internal demands.	LIC1: Sabotage	Deliberate actions aimed to cause disruption or damage to information and/or IT assets for financial or personal gain.
	LIC2: Terrorism	The use of violence to create terror among masses of people; or fear to achieve a financial, political, religious or ideological aim.
	LIC3: Vandalism	Deliberate destruction or damage to information and/or IT assets but, not for personal gain.
	LIC4: Warfare	Damage to assets, facilities, and employees due to war or armed conflict.
Misappropriation: Dishonestly or unfairly taking for one's own use.	LIM1: Embezzlement	To appropriate something, such as property entrusted to one's care fraudulently to one's own use. A form of theft through fraud.
	LIM2: Extortion	The act of obtaining money, property, or services from an organization through coercion. A form of theft through use of force or intimidation to obtain compliance.
	LIM3: Fraud	Deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right.
	LIM4: Theft	The act of logically stealing and/or removing of the property with intent to deprive the rightful owner of it.
Nefarious: Flagrant breaching of time-honored laws and traditions of conduct.	LIN1: Abuse of authorizations	Using authorized access to perform illegitimate actions.
	LIN2: Address Space hijacking	The illegitimate takeover of groups of IP addresses.
	LIN3: Alteration of software	Unauthorized modifications to code or configuration data, attacking its integrity.
	LIN4: Anonymous proxies	Access of web sites through chains of HTTP proxies (obfuscation), bypassing the security mechanism(s).
	LIN5: Autonomous System hijacking	Overtaking, by the attacker, the ownership of a whole autonomous system and its prefixes despite origin validation
	LIN6: Brute force	Unauthorized access via systematically checking all possible keys or passwords until the correct one is found.

- Threat Type is Logical
- Threat Category is Intentional
- Threat Sub-categories are:
  - Conflict
  - Misappropriation
  - Nefarious
- Within the Threat Sub-category of Conflict, there are four (4) Threats
  - Sabotage
  - Terrorism
  - Vandalism
  - Warfare
- Sabotage has a Threat Number of LIC1
  - "L" is for Logical
  - "I" is for Intentional
  - "C" is for Conflict
  - "1" indicates it's the 1st threat in the Sub-category
- Sabotage is defined as "deliberate actions aimed to cause disruption or damage to information and/or IT assets for financial or personal gain."

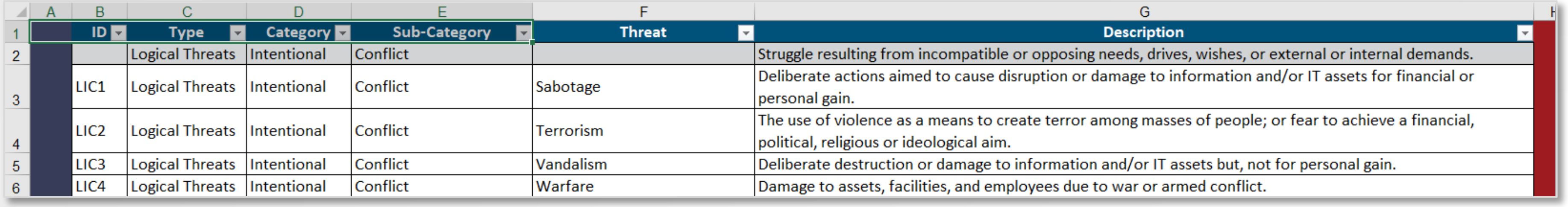
HITRUST Threat Catalogue (1)

The HITRUST Threat Catalogue itself is provided as a Microsoft Excel spreadsheet with seven (7) worksheets:

- Introduction
- Change History
- Definitions
- Consolidated Threats (Pivot)
- Consolidated Threats (Merged)
- Mappings
- Metadata

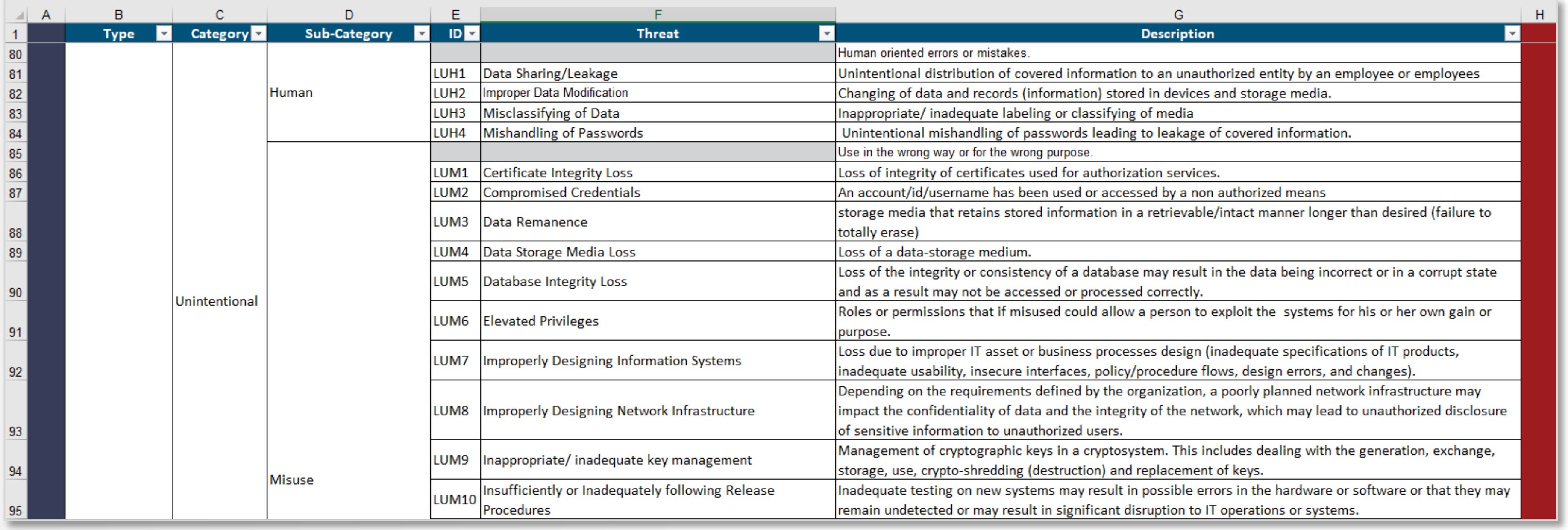
The Consolidated Threats (Pivot) and Consolidated Threats (Merged) worksheets provide the same information as what is presented in the HITRUST Enumerated Threat List.

- The Pivot worksheet provides a simple list in tabular form that can also be filtered for basic analysis
- The Merged worksheet provides a more structured list that is, in many aspects, similar to the table provided in the HITRUST Enumerated Threat List



	A	B	C	D	E	F	G
1		ID	Type	Category	Sub-Category	Threat	Description
2			Logical Threats	Intentional	Conflict		Struggle resulting from incompatible or opposing needs, drives, wishes, or external or internal demands.
3		LIC1	Logical Threats	Intentional	Conflict	Sabotage	Deliberate actions aimed to cause disruption or damage to information and/or IT assets for financial or personal gain.
4		LIC2	Logical Threats	Intentional	Conflict	Terrorism	The use of violence as a means to create terror among masses of people; or fear to achieve a financial, political, religious or ideological aim.
5		LIC3	Logical Threats	Intentional	Conflict	Vandalism	Deliberate destruction or damage to information and/or IT assets but, not for personal gain.
6		LIC4	Logical Threats	Intentional	Conflict	Warfare	Damage to assets, facilities, and employees due to war or armed conflict.

Example: Consolidated Threats (Pivot) Worksheet



	A	B	C	D	E	F	G
1		Type	Category	Sub-Category	ID	Threat	Description
80			Unintentional	Human			Human oriented errors or mistakes.
81					LUH1	Data Sharing/Leakage	Unintentional distribution of covered information to an unauthorized entity by an employee or employees
82					LUH2	Improper Data Modification	Changing of data and records (information) stored in devices and storage media.
83					LUH3	Misclassifying of Data	Inappropriate/ inadequate labeling or classifying of media
84					LUH4	Mishandling of Passwords	Unintentional mishandling of passwords leading to leakage of covered information.
85				Misuse			Use in the wrong way or for the wrong purpose.
86					LUM1	Certificate Integrity Loss	Loss of integrity of certificates used for authorization services.
87					LUM2	Compromised Credentials	An account/id/username has been used or accessed by a non authorized means
88					LUM3	Data Remanence	storage media that retains stored information in a retrievable/intact manner longer than desired (failure to totally erase)
89					LUM4	Data Storage Media Loss	Loss of a data-storage medium.
90					LUM5	Database Integrity Loss	Loss of the integrity or consistency of a database may result in the data being incorrect or in a corrupt state and as a result may not be accessed or processed correctly.
91					LUM6	Elevated Privileges	Roles or permissions that if misused could allow a person to exploit the systems for his or her own gain or purpose.
92					LUM7	Improperly Designing Information Systems	Loss due to improper IT asset or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors, and changes).
93					LUM8	Improperly Designing Network Infrastructure	Depending on the requirements defined by the organization, a poorly planned network infrastructure may impact the confidentiality of data and the integrity of the network, which may lead to unauthorized disclosure of sensitive information to unauthorized users.
94					LUM9	Inappropriate/ inadequate key management	Management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys.
95					LUM10	Insufficiently or Inadequately following Release Procedures	Inadequate testing on new systems may result in possible errors in the hardware or software or that they may remain undetected or may result in significant disruption to IT operations or systems.

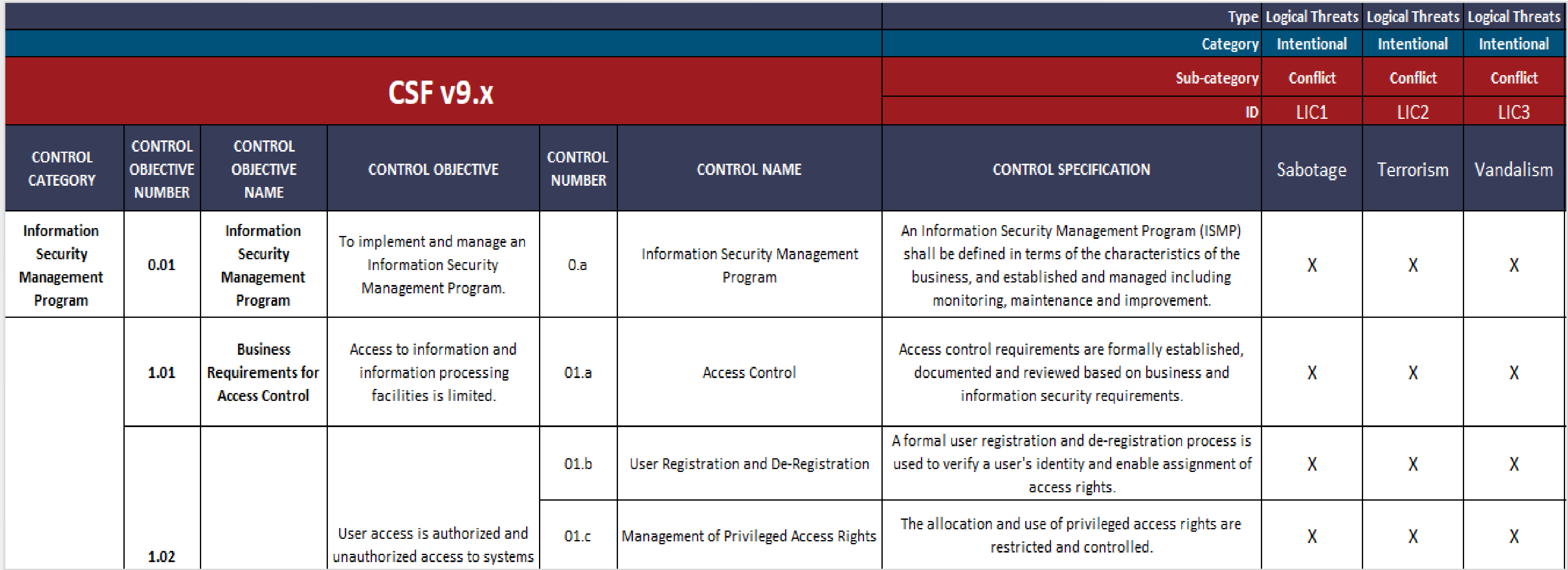
Example: Consolidated Threats (Merged) Worksheet

HITRUST Threat Catalogue (2)

The principal resource in the HITRUST Threat Catalogue is the Mappings Worksheet, as it provides:

- HITRUST CSF v9.4.x
  - Control Categories
  - Control Objective Numbers
  - Control Objective Names
  - Control Objectives
  - Control Number
  - Control Name
  - Control Specification/Description
- Mappings to all the Catalogue's enumerated threats, including their metadata, such as:
  - Threat Type
  - Threat Category
  - Threat Sub-category
  - Threat Number
  - Threat Name

The Metadata worksheet (not shown) provides coverage mappings of some external catalogues.



CSF v9.x						Type	Logical Threats	Logical Threats	Logical Threats
						Category	Intentional	Intentional	Intentional
						Sub-category	Conflict	Conflict	Conflict
						ID	LIC1	LIC2	LIC3
CONTROL CATEGORY	CONTROL OBJECTIVE NUMBER	CONTROL OBJECTIVE NAME	CONTROL OBJECTIVE	CONTROL NUMBER	CONTROL NAME	CONTROL SPECIFICATION	Sabotage	Terrorism	Vandalism
Information Security Management Program	0.01	Information Security Management Program	To implement and manage an Information Security Management Program.	0.a	Information Security Management Program	An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance and improvement.	X	X	X
	1.01	Business Requirements for Access Control	Access to information and information processing facilities is limited.	01.a	Access Control	Access control requirements are formally established, documented and reviewed based on business and information security requirements.	X	X	X
	1.02		User access is authorized and unauthorized access to systems	01.b	User Registration and De-Registration	A formal user registration and de-registration process is used to verify a user's identity and enable assignment of access rights.	X	X	X
				01.c	Management of Privileged Access Rights	The allocation and use of privileged access rights are restricted and controlled.	X	X	X

Example: Mappings Worksheet

Section 4

WHAT ARE THE GOALS AND BENEFITS?

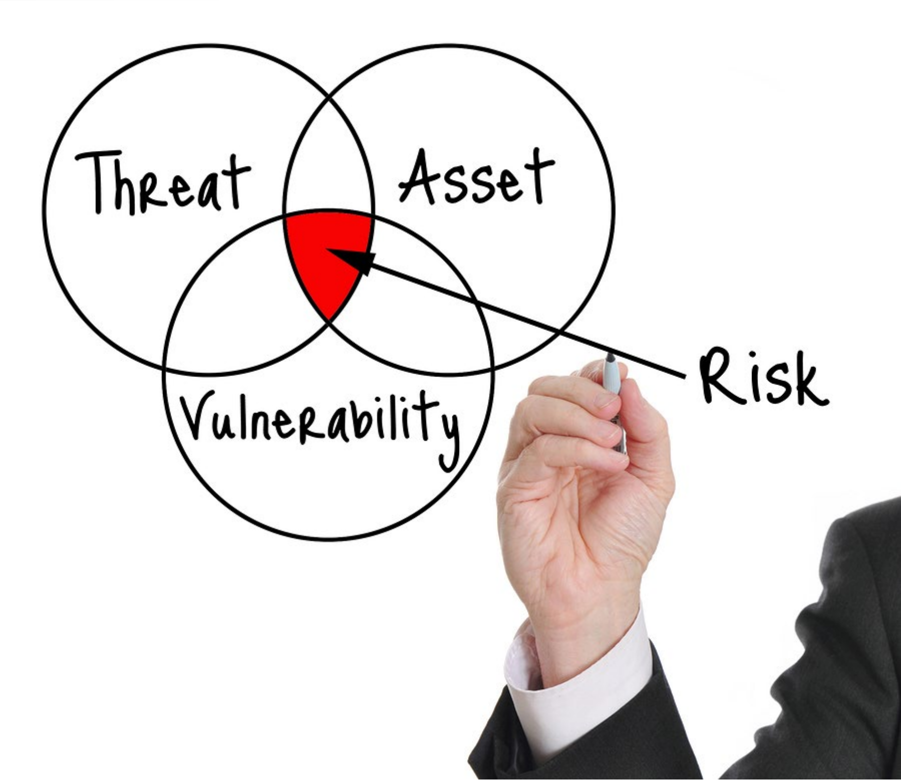
Goals and Benefits

The HITRUST Threat Catalogue is designed to aid organizations in improving their information security posture by better aligning cyber threats with HITRUST CSF control requirements. The explicit alignment of threats to the HITRUST CSF produces a combination not found in other frameworks. It helps simplify the risk analysis process and reduces some of the burden, costs, and confusion otherwise experienced when attempting to achieve this level of analysis.

Identifying threats is a major component of a comprehensive risk analysis process for any organization seeking to protect their sensitive data and helps determine what adverse events are relevant to the organization and must be controlled. For example, the increased frequency of ransomware attacks has prompted many organizations to re-examine their controls around data backup and restoration and ensure they could successfully recover their data if an attack occurred.
The HITRUST Threat Catalogue also provides greater visibility into areas representing the greatest risk exposure and enhances the underlying risk analyses used to develop the HITRUST CSF.

More specifically, the HITRUST Threat Catalogue is intended to help organizations, regardless of industry, domestic or international, to:

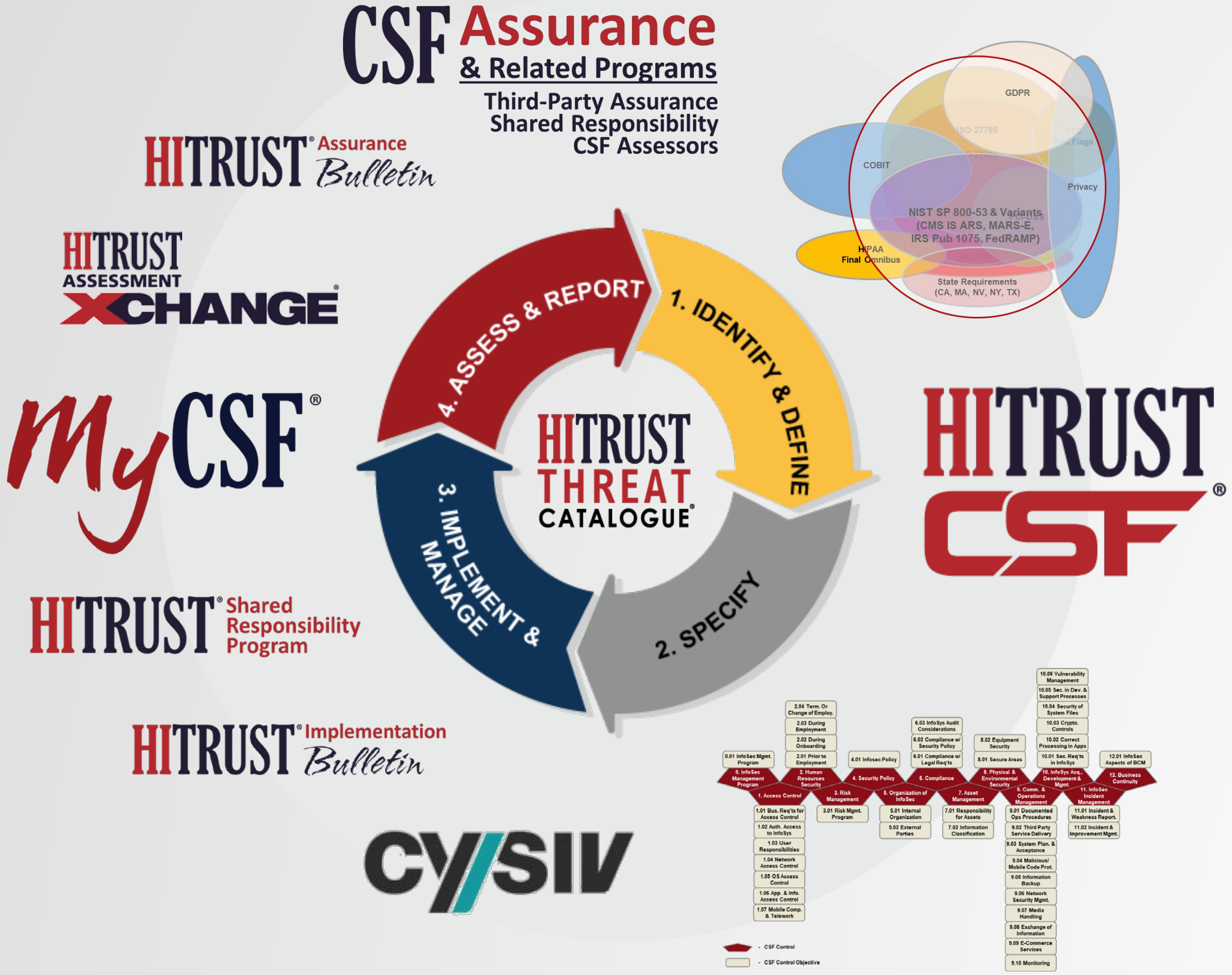
- Identify all “reasonably anticipated” threats
- Conduct multiple types of risk analyses
  - *General HIPAA risk analysis for initial control selection*
  - *Supplemental analyses for tailoring of the control baseline*
  - *Targeted analyses for risk acceptance and alternate control selection*
- Consume threat intelligence
  - *Threat advisories tied to the controls intended to help address them*
  - *Allows organizations to review their readiness/preparedness as the threat environment changes*
- Help HITRUST
  - *Maintain currency and relevance of HITRUST CSF controls*
  - *Maintain alignment of implementation requirements with increasing levels of risk*



Section 5

HOW DOES IT RELATE TO THE HITRUST SUITE OF PROGRAMS AND SERVICES?

Relationship to the HITRUST Approach



CSF Assurance & Related Programs
Third-Party Assurance
Shared Responsibility
CSF Assessors
HITRUST Assurance Bulletin
HITRUST ASSESSMENT XCHANGE
MyCSF
HITRUST Shared Responsibility Program
HITRUST Implementation Bulletin
CYSIV
HITRUST THREAT CATALOGUE
1. IDENTIFY & DEFINE
2. SPECIFY
3. IMPLEMENT & MANAGE
4. ASSESS & REPORT
GDPR
ISO 27799
COBIT
Privacy
NIST SP 800-53 & Variants (CMS IS ARS, MARS-E, IRS Pub 1075, FedRAMP)
HIPAA Final Omnibus
State Requirements (CA, MA, NV, NY, TX)
HITRUST CSF
CSF Control
CSF Control Objective

The HITRUST Threat Catalogue is an integral part of the risk management programs and services that support the HITRUST Approach. Specifically, the Threat Catalogue:

- Helps maintain the currency and relevancy of the HITRUST CSF framework by providing better visibility into how extant and emerging threats are addressed by specific HITRUST CSF control requirements
- Allows for better tailoring of an organization’s HITRUST CSF control baseline—selected based on its organizational, system (technical), and regulatory (authoritative) risk factors
- Supports “real-time” updates to implemented controls for users of the HITRUST CSF, thereby supporting better threat management
- Helps prioritize corrective actions to better address a dynamic threat environment
- Provides better support for continuous monitoring of HITRUST CSF controls and the sharing of associated risk information with internal and external stakeholders

Section 6

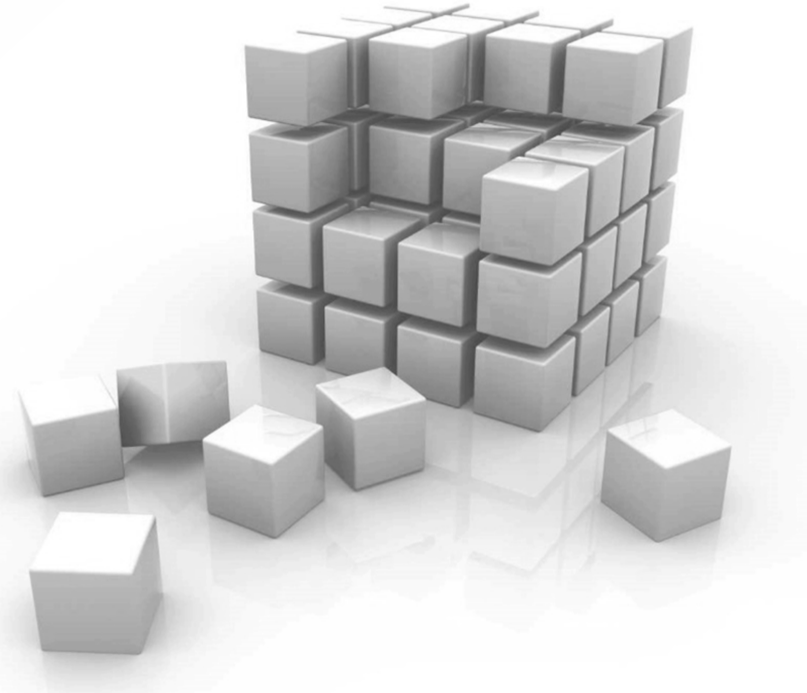
HOW WILL IT CONTINUE TO EVOLVE AND IMPROVE?

Development Approach

HITRUST's primary objective is for the Threat Catalogue to be leveraged (1) by HITRUST to maintain the HITRUST CSF and (2) by organizations to better facilitate the consumption of threat intelligence and support general risk analysis requirements. HITRUST expects development of the Threat Catalogue will require multiple iterations to ensure it can satisfy this objective.

- HITRUST Threat Catalogue 1.0.1 (Q3 2021)
  - Updated HITRUST CSF control mappings to the Ransomware threat based on updated guidance from CISA
- HITRUST Risk Catalogue 2.0 release (Q1/Q2 2022)
  - Update threat taxonomy, enumerated threats, and threat definitions based on:
    - Industry feedback
    - HITRUST MAE WG recommendations
    - Support for quasi-quantitative risk analysis
  - Map threats to HITRUST CSF v9.x.x control requirements
  - Add FAIR-CAM control attribute metadata for HITRUST CSF control requirements
  - Release for public comment (60 days)
- HITRUST Risk Catalogue 3.0 release (Q2/Q3 2022)
  - Update threat taxonomy, enumerated threats, and threat definitions based on:
    - Industry feedback
    - Additional support for quasi-quantitative risk analysis, if needed
  - Update HITRUST CSF v9.x.x control requirements' mappings to enumerated threats based on industry feedback
  - Add threat/control metadata to support new approach to quasi-quantitative risk analysis (e.g., vulnerability classes and asset types)
  - Release for public comment (60 days)
- Additional Work on the Roadmap
  - Develop supporting guidance on how to leverage the Catalogue for supplemental and targeted risk analyses
  - Explore/Develop approach to augment threat intelligence with information from the HITRUST Threat Catalogue
  - Identify further areas of improvement and/or additional development

"Perfect is the enemy of good."



Section 7

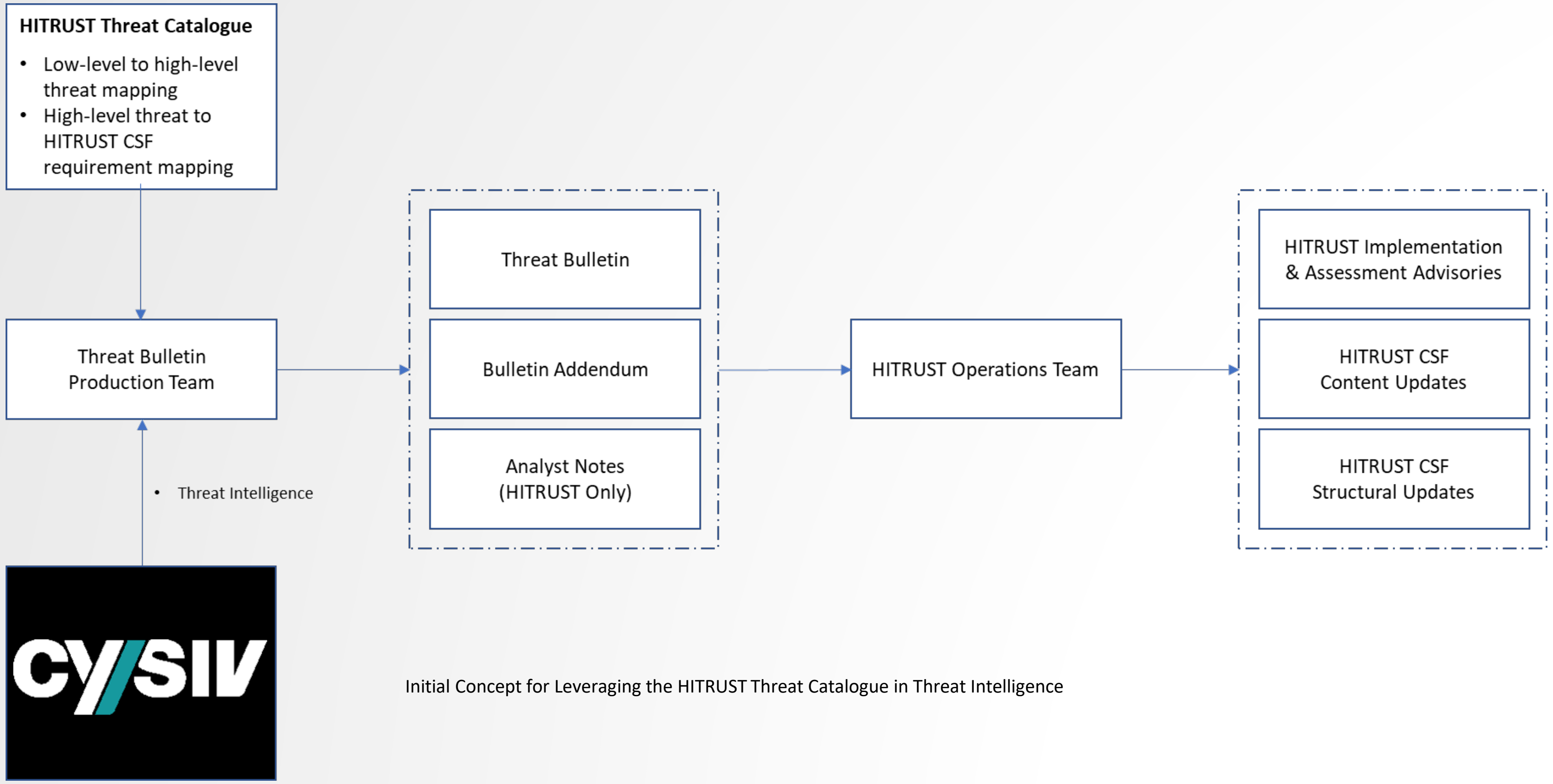
WHAT OTHER QUESTIONS ARE FREQUENTLY ASKED?

Frequently Asked Questions (1)

FAQ	Response
1. How do I explain the HITRUST Threat Catalogue to my executives?	The HITRUST Threat Catalogue provides a comprehensive list of threats to PII (including ePHI) and other types of sensitive information and maps these threats to the HITRUST CSF v9.4.x controls intended to address them. This allows HITRUST to better align HITRUST CSF requirements with emerging threats, increasing its value in risk mitigation while simplifying an organization's selection of security controls. In addition, the HITRUST Threat Catalogue helps organizations gain better visibility into how they manage information security risk and supports better prioritization of security-related investments, including the remediation or enhancement of existing controls as well as the implementation of new controls.
2. How does the HITRUST Threat Catalogue make the HITRUST CSF better or improve its ability to help manage risk?	By identifying and mapping threats to HITRUST CSF controls based on their specifications, HITRUST gains additional visibility into how the controls mitigate associated risk. This helps ensure the risks associated with specific threats are addressed appropriately, including any increased risk due to an organization's specific risk factors. For example, organizations that are large, complex, or aggregate large amounts of information generally present more risk, e.g., due to a larger attack surface or increased threat actor motivation, would generally require more robust controls.
3. Does HITRUST have a working group (WG) to help develop the Threat Catalogue and, if so, how can I get involved?	HITRUST intends to re-establish the HITRUST Threat Catalogue WG sometime in Q3 or early Q4 2021 to support continued development. The HITRUST community can expect a 'call for participation' at that time, and anyone interested in supporting this effort will be able to request consideration for membership via our Working Group sign-up page.

Frequently Asked Questions (2)

FAQ	Response
4. When will cyber threat intelligence be linked to the threats in the HITRUST Threat Catalogue?	Once the mappings between threats and HITRUST CSF controls are completed, HITRUST will begin exploring ways to relate these mappings to the more granular threats identified in active threat intelligence. An initial concept for this type of integration, working with one of our HITRUST partners, is provided in the figure below.



HITRUST Threat Catalogue
Low-level to high-level threat mapping
High-level threat to HITRUST CSF requirement mapping
Threat Bulletin Production Team
Threat Intelligence
CYSIV
Threat Bulletin
Bulletin Addendum
Analyst Notes (HITRUST Only)
HITRUST Operations Team
HITRUST Implementation & Assessment Advisories
HITRUST CSF Content Updates
HITRUST CSF Structural Updates

Initial Concept for Leveraging the HITRUST Threat Catalogue in Threat Intelligence

Frequently Asked Questions (3)

FAQ	Response
5. Will all the threats to personal data be listed in the HITRUST Threat Catalogue?	The HITRUST Threat Catalogue is focused on providing as comprehensive a list as possible. However, users of the HITRUST Threat Catalogue should keep in mind that the threats are enumerated at a level consistent with the control specification in the HITRUST CSF. Intelligence generally specifies threats at a much more granular level.
6. How will the HITRUST Threat Catalogue evolve over time?	The HITRUST Threat Catalogue is a "living document" due to the constantly changing threat environment, and as such, includes planned improvements to better facilitate risk analyses and the consumption of threat intelligence. Changes will likely include modifying the threat list, enumerating common vulnerabilities, relating Indicators of Compromise (IOCs), and of course updating control requirements as they change with each HITRUST CSF release.
7. How does the HITRUST Threat Catalogue help me perform a risk analysis?	By understanding how HITRUST CSF controls address specific threats to personal data and other sensitive information, an organization can demonstrate the results of the risk analyses used by the underlying control frameworks in the HITRUST CSF, e.g., ISO 27002, NIST SP 800-53, and PCI-DSS, as well as support other types of risk analyses. For example, organizations will be able to support further tailoring of the HITRUST CSF control baseline generated from its organizational, system, and regulatory risk factors by (1) addressing any additional or unique threats or vulnerabilities it may have, which may not be addressed by a HITRUST CSF control requirement in the HITRUST Threat Catalogue, (2) supporting the appropriate and allowable selection of alternative or compensating controls that are not contained in the HITRUST CSF, and/or (3) the removal or relaxation of specific control requirements in its baseline to help ensure the most cost-effective, risk-based application of the HITRUST CSF to its business and clinical environment. References: i. ISO/IEC 27002:2013, available at http://www.iso.org/iso/catalogue_detail?csnumber=54533 ii. NIST SP 800-53 r5, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf iii. PCI DSS v3.1, available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

Frequently Asked Questions (4)

FAQ	Response
8. Will the HITRUST Threat Catalogue help me with HIPAA compliance?	By enumerating common threats and, when available, common vulnerabilities, an organization will have additional information to support a risk analysis consistent with NIST and HHS recommendations, which require an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [ePHI]" (HIPAA § 164.308(a)(1)(ii)(A)) and "protect[ion] against any reasonably anticipated threats or hazards to the security or integrity of [such information]" (HIPAA § 164.306(a)(2)). Today, HITRUST does this by tailoring an industry-level overlay of the NIST SP 800-53 moderate-impact minimum security baseline and leveraging the risk assessments used to develop the HITRUST CSF's underlying frameworks. The HITRUST Threat Catalogue will help provide an additional level of granularity by showing the relationship between the control requirements specified in the HITRUST CSF with a list of 'reasonably anticipated threats.' References: i. HIPAA Administrative Simplification Regulation Text, available at https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf ii. NIST SP 800-30 r1, available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf iii. HHS Guidance on Risk Analysis Requirements under the HIPAA Security Rule, available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
9. How does threat intelligence being linked to the HITRUST CSF help me better protect health information?	By linking granular threats identified in active threat intelligence to (1) higher-level threats contained in the HITRUST Threat Catalogue and (2) related HITRUST CSF controls, organizations will gain greater insight into how well they are addressing extant and emerging threats by evaluating how well they've implemented related HITRUST CSF controls in their environment.
10. How will HITRUST use threat intelligence to update the requirements in the HITRUST CSF?	By understanding the control requirements in the HITRUST CSF that are intended to address specific threats identified in threat intelligence, HITRUST will gain greater insight into how they are adequately addressed based on current industry-accepted (aka "best") practices. If more robust controls or enhancements are needed to adequately address the threat(s), then HITRUST would issue an Implementation Advisory to raise awareness and formally update related HITRUST CSF requirements in its next release.

Frequently Asked Questions (5)

FAQ	Response
11. What would prompt HITRUST to issue additional HITRUST CSF implementation guidance?	A HITRUST Advisory would be issued if there is additional clarification around how HITRUST CSF requirements should be implemented to effectively address one or more threats—or as an interim measure until more stringent or enhanced control requirements can be published in the next scheduled release of the HITRUST CSF.
12. How often will the HITRUST Threat Catalogue be updated?	We anticipate updates to occur annually, shortly after each HITRUST CSF release, or when significant changes in the threat environment would warrant an interim release.

HITRUST®

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the
Content Spotlight