Security Frameworks

Chris Hoofnagle

For the California Privacy Protection Agency

March 30, 2022

Four points

1. Security terms of art

   Why important: easy to misunderstand industry bc of terminology

2. Policy goals and instruments; frameworks are instruments

   Why important: instruments attract more attention than goals

3. Harmony in security frameworks

   Why important: there is high-level congruency on security hygiene

4. Mechanisms to implement security frameworks

   Why important: the mechanisms vary from self-selection to prescription

1. Terms of art in security

- Audit: examination of practices against an externally-defined standard
- Assessment: an expert opinion on company-identified goals
  - Most security evaluations are *assessments* not *audits*
  - Evidentiary requirement: assessor must find “sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.”
  - Product could be a 1-page-long letter (think about evidence)
- Security incident: an event that indicates a problem in CIA
  - A security incident may not require notification
- Security breach: a legal determination that a security incident requires notification
- ”Accountable” has two meanings: the ability to *make an accounting*, and accountability in the sense of *responsibility*

2. Policy goals --- our *terminal goals*

- CPRA Preamble: “K. Business should also be **held directly accountable** to consumers **for data security breaches** and **notify** consumers when their most sensitive information has been **compromised**.”
- “A business that collects a consumer’s personal information shall **implement reasonable security procedures** and practices appropriate to the **nature** of the personal information to protect the personal information from **unauthorized or illegal access, destruction, use, modification, or disclosure** in accordance with Section 1798.81.5.” (1798.100)
- ”Security” has broad meaning (1798.140)
  - Referent object: individuals’ personal information
  - Threats: security *incidents*, CIA

Goals and instruments: incentive conflicts

- CCPA is a *rights-based* framework that concretizes the State's Art 1 § 1 *value* placed on privacy
- Governments' legitimacy comes from securing rights
- Companies' legitimacy comes from commercial utility
  - Companies' lodestar is *risk* not *values*
  - Companies operationalize security through controls
  - Documentation of these controls are just as important as doing them
  - **Companies may elevate the instrument to a terminal value**
    - That is, while the public policy goal is to secure personal information, companies may convert this into a terminal goal of demonstrating compliance with a security framework

	Knowns	Unknowns
Known	Many security breaches are reported by controllers of personal information Root causes frequently are simple errors & accidents	No one knows the extent of undiscovered incidents surrounding PI and IP
Unknown	Companies know the extent of undisclosed incidents of PI* and of intellectual property incidents but regulators do not *In 2020, Constella Intelligence (a company I advise) found 8,500 dark web leakages	???

A regulatory vision:

How might policy move us out of the known knowns and elucidate and prevent hidden or undiscovered incidents?

Vision: Conceiving of security

A negligence model (current)

- Encourage “reasonable” precautions
- Focus on “injury,” “wrongfulness” == devote resources to evaluating adequacy of company conduct
- Companies & consumers share costs of incidents

An enterprise liability model (possible target model)

- Companies benefit from collecting PI; they should bear the burdens
- Presume incidents reflect wrongful practices
- Focus on deterrence, making consumers whole == devote resources to detection, enforcement

A Maturity Model

2022

- Focus on breadth: ensure all collectors of PI are assessing risks
- Mechanisms: perhaps a lightweight certification & retention requirement

2025+

- Focus on depth: ensure assessments follow evolving standard of care
- Mechanisms: spot checks; release of examples of high-quality assessment

2030+

- Focus on accountability: companies own full risk of incidents
- Mechanisms: shift to deterrent enforcement

3. The harmony in security frameworks

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9,

From the NIST Cybersecurity Framework (version 1.1): Identity Function

Five “functions” are activities to promote cybersecurity.
“ID” activities “Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.”

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9,

Categories decompose the functions to specific steps
Even the most basic subcategory: identification of devices, is complicated

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9,

Informative references show how NIST's precautions map onto other standards.
Key point: there is great congruence among security standards.
Key point: mappings create universality. This is of central importance to businesses.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9,

4. Mechanisms of frameworks differ

- Framework-based: company free to choose precautions based on a menu of approaches
  - NIST Cybersecurity Framework
- Process-based: company specifies processes & goals
  - ISO 270XX (client defines the goals, examiner assesses processes)
- Controls-based: company must have controls, but has some flexibility in implementing them
  - NIST SP 800-53 Rev. 5
- Requirements-based: client must do x, y, and z
  - PCI-DSS (card acceptance) most prescriptive

Slide appendix

Portable Compliance Profile™

Authority Documents

- 9070 - NFA Compliance Rules 2-9, 2-36 and 2-...
- Cloud Computing Compliance Controls Catal...
- CobiT
- FFIEC Business Continuity Planning (BCP) IT E...
- Hong Kong Monetary Authority: TM-G-1: Gen...
- IM Guidance Update: Cybersecurity Guidance
- ISO 22301: Societal Security - Business Contin...
- ISO 24762 Information technology - Security t...
- ISO/IEC 27018:2014, Information technology ...
- National Initiative for Cybersecurity Educatio...
- Payment Card Industry (PCI) Data Security St...
- Shared Assessments Standardized Informati...

Continuity-Heavy Authority Documents

KEY **1848 Mandated** *206 Implied*

Control Name	ID #
Leadership and high level objectives	00597
Audits and risk management	00677
Monitoring and measurement	00636
Technical security	00508
Physical and environmental protection	00709
Operational and Systems Continuity	00731
Establish and maintain a business continuity program.	13210
Establish and maintain a pandemic plan.	13214
Prepare the alternate facility for an emergency offsite relocation.	00744
Train personnel on the continuity plan.	00759
Test the continuity plan, as necessary.	00755
Implement the continuity plan, as necessary.	10604
Review and update the continuity plan.	00754
Human Resources management	00763
Establish and maintain high level operational roles and responsibil...	00806
Assign the roles and responsibilities of management in establis...	13112

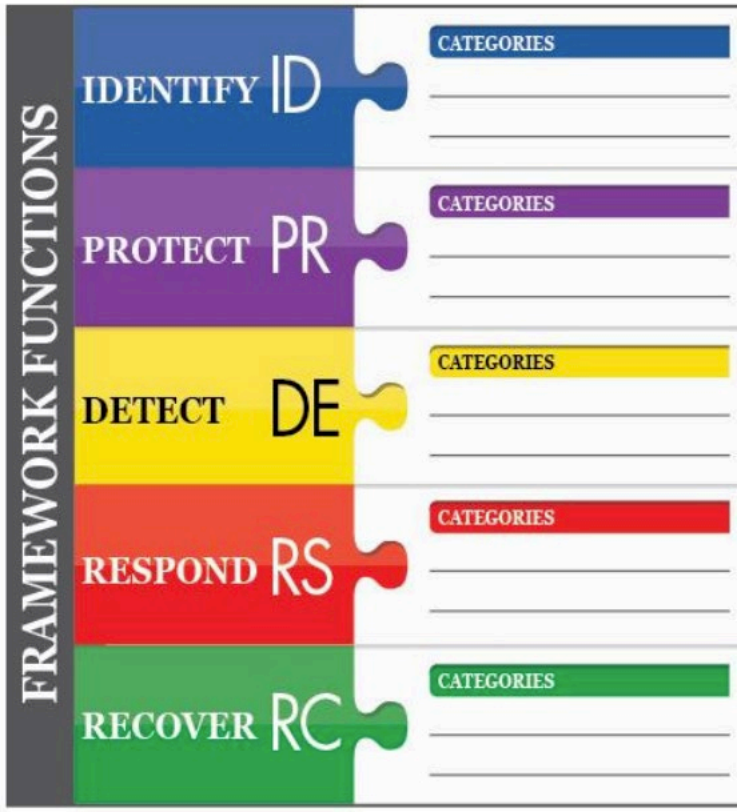
Companies may be subject to multiple frameworks and attempt to implement controls that satisfy all of them.

From Unified Compliance

ISO 27000-XX

- Not necessarily for IT companies
- Leaves a lot to company, auditor to define processes
  - Need to look into specifics to assess its quality
  - Maybe schedule more frequent review (6 months)
- Establishes a high-level vocabulary for security, enumerates lists of control areas
- Well established in Asia, use cases:
  - Outsourcing (non-payment environment), data processing
  - So flexible that it is used in many different industries (even health, banking)
- Cannot say 100% secure—assessor says there is a “reasonable” amount of compliance

The NIST Framework Core



Identify what needs to be protected

Select and implement safeguards

Implement mechanisms to sense incidents

Mechanisms to mitigate incidents

Restore or be resilient to attacks

The NIST Framework is voluntary, it is risk-based, and it is popular even among startup companies because of its flexibility. Downside: flexibility = companies could choose poorly.

PCI-DSS

- Attempts to make a widely-shared number secret
- Highly prescriptive
- 12 high level goals
- Over 100 requirements

NIST 800-53

- Developed by federal government, controls for info and info systems
  - Need to comply if you want to be federal govt contractor
  - May be good for thinking through strategy
  - Reflects priorities of government—accountability, amenable to supervision
  - Is intel community outside these requirements?
- Based on “CIA” confidentiality, integrity, availability
- Big picture: risk management, technology-neutral; auditing & measuring in complex hierarchy
  - Now includes some fair information practices
- Evaluate importance of systems
- Requirements are high-level on first read
- For these identified risks we can trust this system because of these processes
- Security as continuous process, human process