PCI Compliance as a Security Project

HOW PREPARING FOR PCI AUDIT CAN MAKE AN ORGANIZATION SAFER

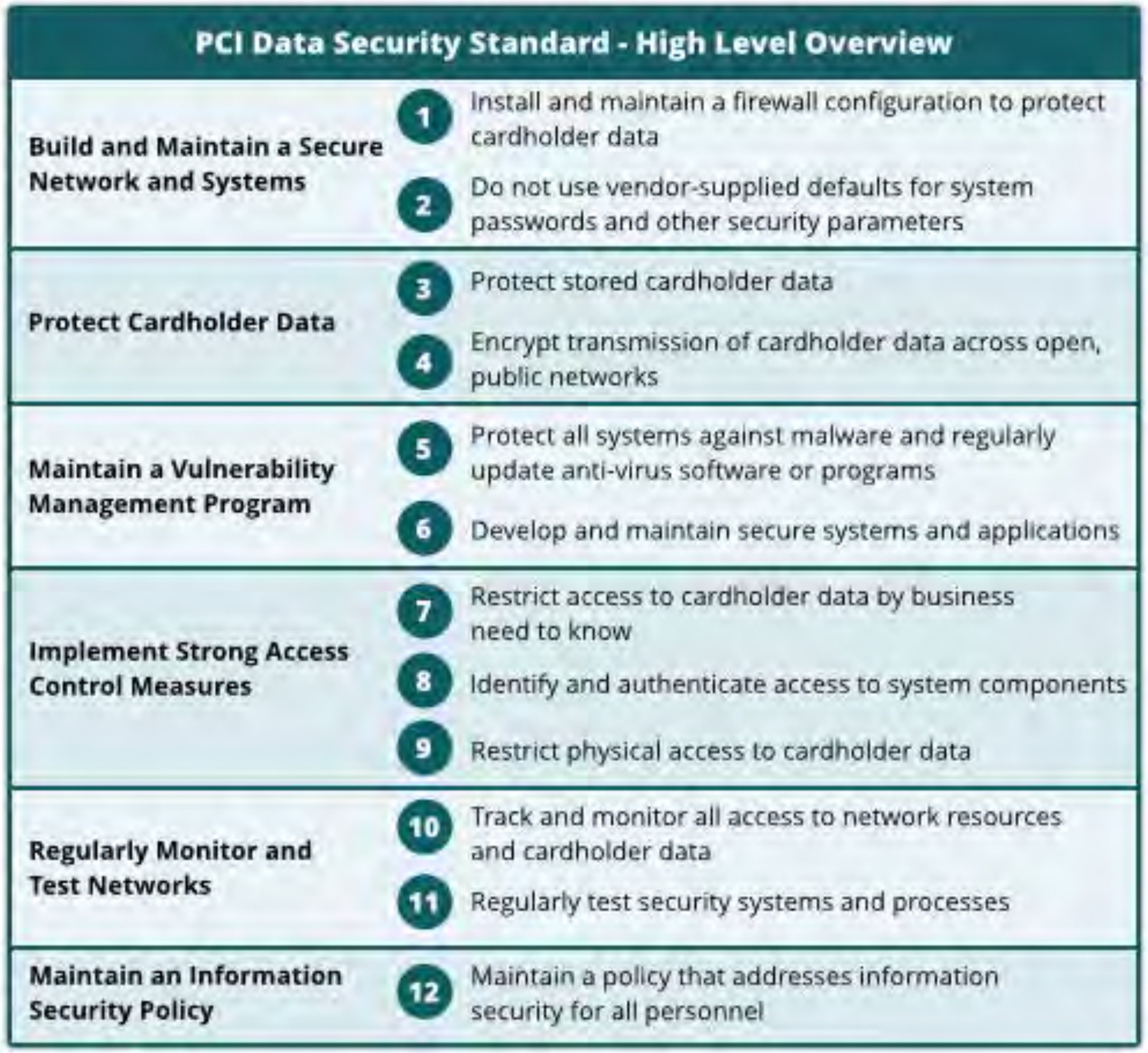
Agenda

- Who is this guy?
- Most PCI requirements are just security directives, however oddly worded.
- Security best practices map to PCI requirements
- A NIST CSF to PCI 4 crosswalk
- How making an org ready for PCI audit improves their security, and vice versa

Who is this guy?

- David C Frier, CISSP, CISM, CRISC, CCSK
- vCISO and Senior Cybersecurity Program Manager at Sedara... *but I speak only for myself, not for Sedara!*
- I’ve been doing Information Security for seventeen years and IT of one sort or another for two score and three
- Avid player of poker, Orioles and Cubs fan, enthusiastic-if-slow rider of a Trek.

Structure of PCI-DSS



PCI Data Security Standard - High Level Overview

Build and Maintain a Secure Network and Systems	1	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5	Protect all systems against malware and regularly update anti-virus software or programs
	6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7	Restrict access to cardholder data by business need to know
	8	Identify and authenticate access to system components
	9	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an Information Security Policy	12	Maintain a policy that addresses information security for all personnel

- 6 Compliance Groups
- 12 “Requirements”
  - Each one is actually a collection of control requirements
- Various applicability depending on the type of organization

PCI-DSS 4 is New

- Recent release of PCI-DSS v4 - phasing in through March ’25
- Fundamental changes from v3.21
- Changes are oriented to improving org security
    - More emphasis on MFA
    - Proper control of generic and service acts
    - Modernized password reqmts.
- And improving org security ***process***
    - Mandating Risk Reviews
    - Reporting improvements

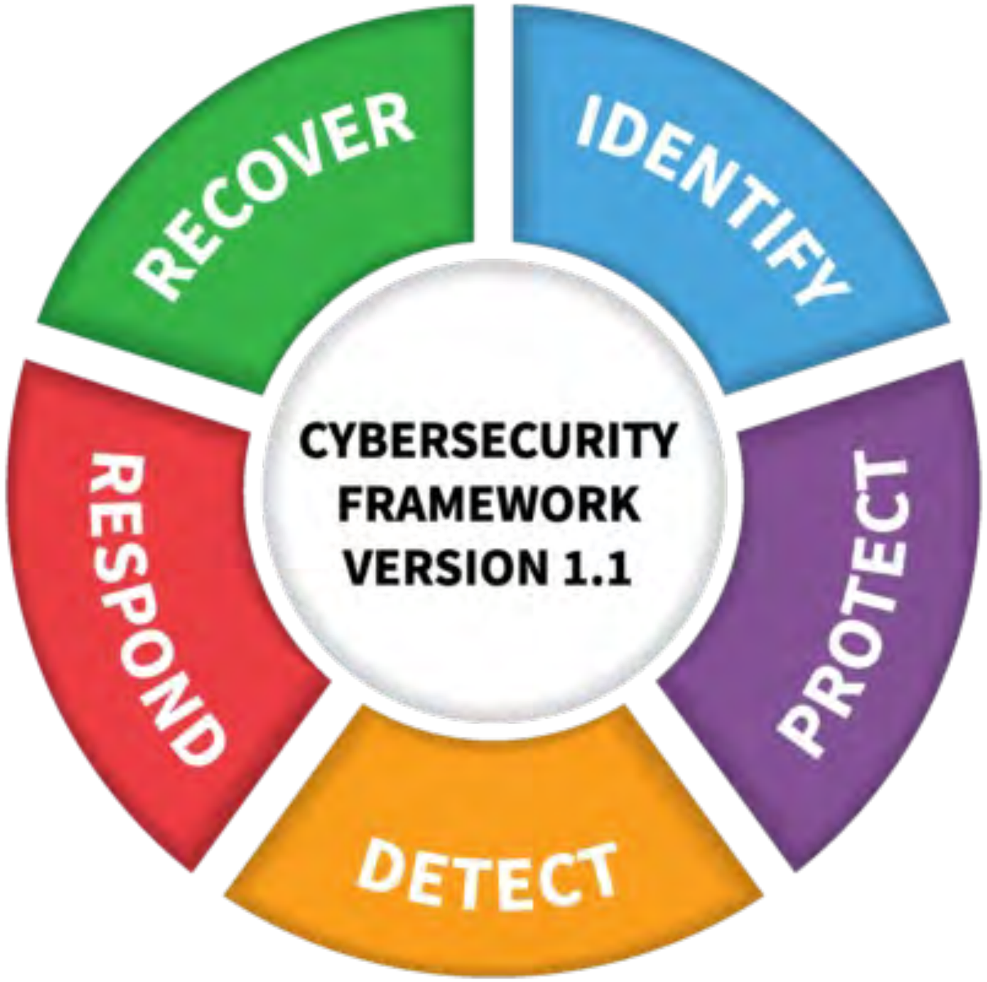
> “PCI-DSS Requirements **ARE** Security Requirements ”
>
> --ME

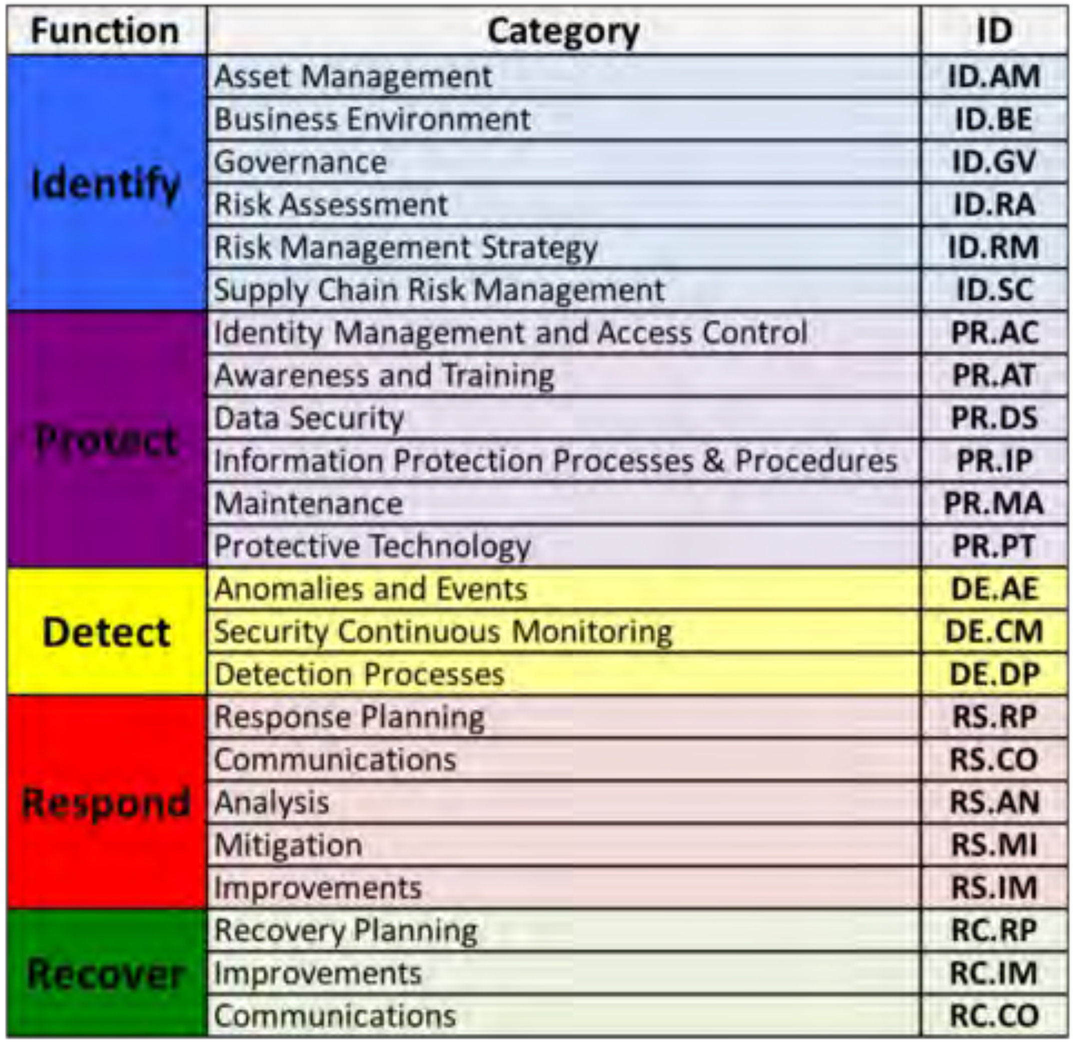
- Effects of DSS 4.0:
  - Modernizing requirements that were outmoded *(e.g. password complexity)*
  - Emphasizing MFA and Monitoring
  - Tightening auditability and process

PCI-DSS 4 Improves Security

- PCI Requirements Will Improve the Org’s Security, if they only follow them
- Follow them in spirit not just in letter….

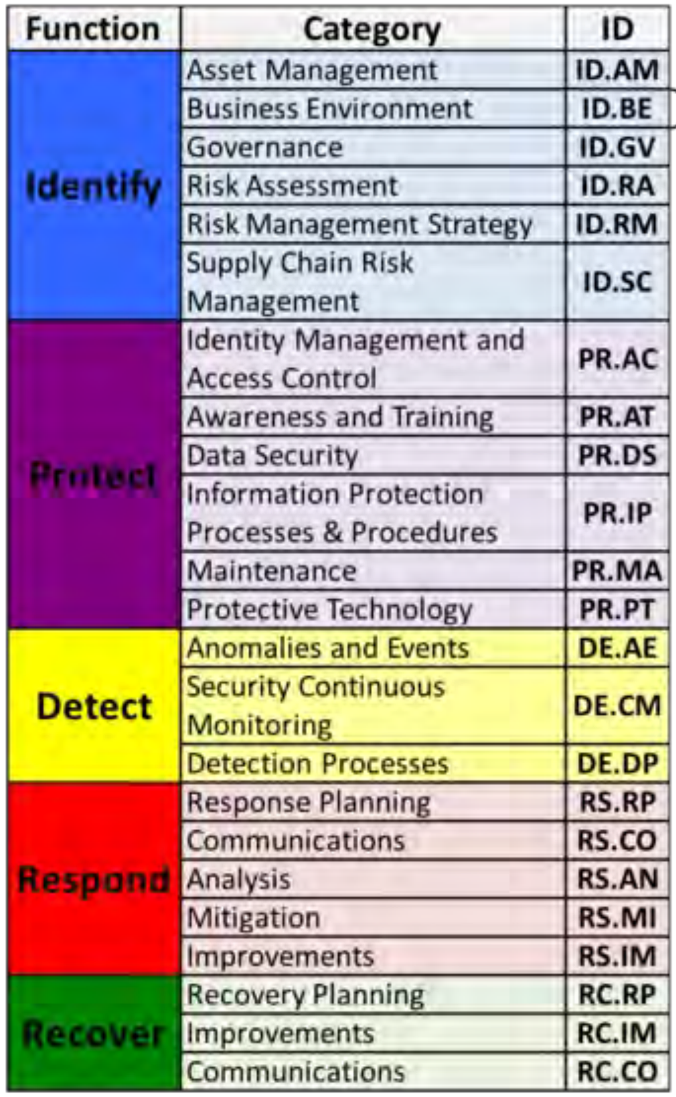
Structure of NIST-CSF



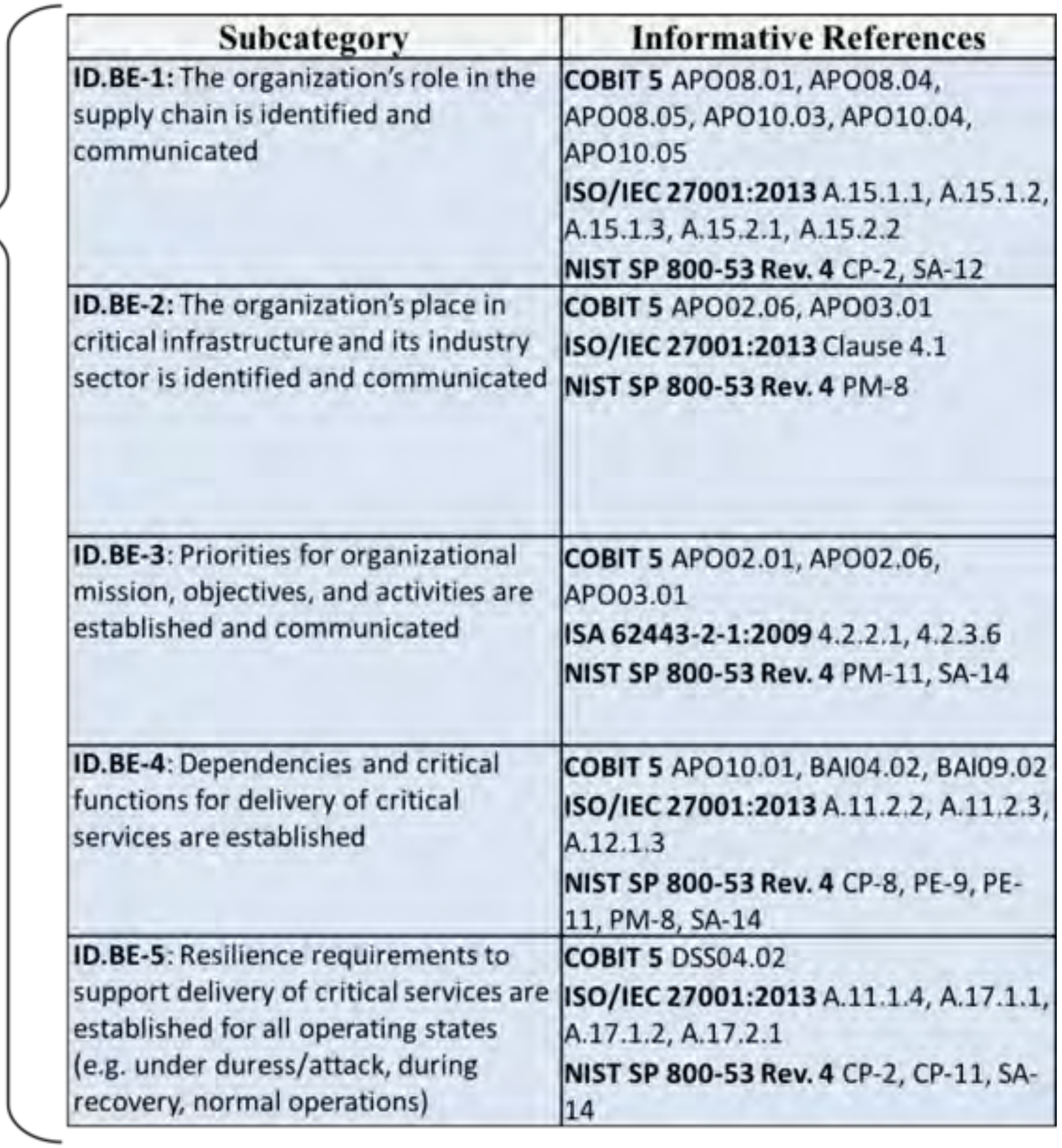


Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Structure of NIST-CSF – *more detail*



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

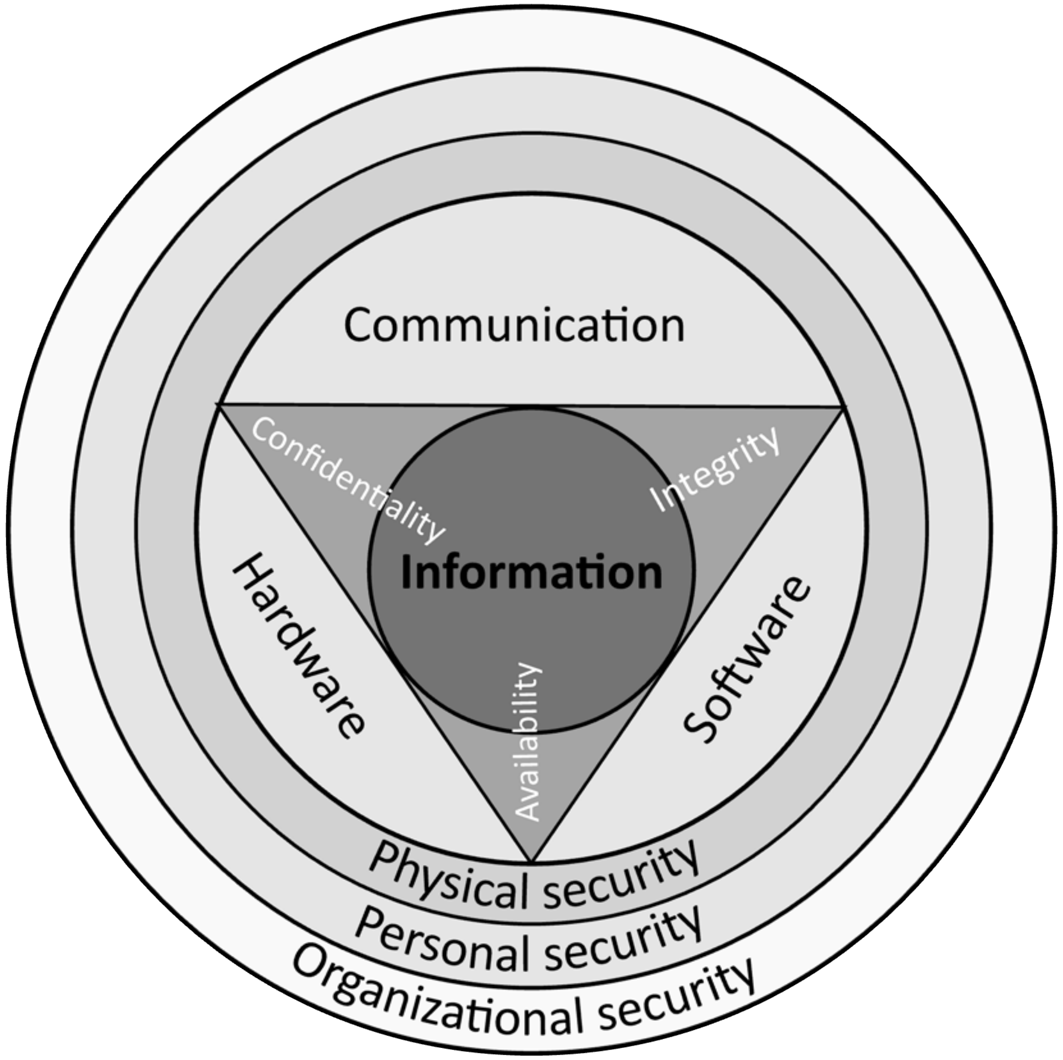


Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

About the Triad

- CIA
  - Confidentiality
  - Integrity
  - Availability
- NIST CSF concerns itself with all three, at least to some extent
- PCI-DSS seems mostly concerned with C, I

This comes up in a bit



Crosswalk

- I have prepared a rough-cut crosswalk of NIST to PCI
- A copy of my spreadsheet will accompany these slides

- Methodology:
  - PCI SS provided a NIST-CSF to PCI-DSS 3.2.1 mapping

    and
  - PCI-DSS 3.2.1 to 4.0 table of changes
  - I extrapolated NIST-CSF subcategories to PCI-DSS 4.0 requirements
  - This mapping is likely imperfect. Use as a general guide only

    Free, and worth every penny

Mapping NIST to PCI

NIST CSF Control	PCI-DSS 4 Requirement
ID.GV-1: Organizational cybersecurity policy is established and communicated	Requirement 12: Support Information Security with Organizational Policies and Programs
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	Requirement 6.3: Security vulnerabilities are identified and addressed.
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction….	Requirement 8.3: Strong authentication for users and administrators is established and managed.
DE.CM-1: The network is monitored to detect potential cybersecurity events	Requirement 10.4: Audit logs are reviewed to identify anomalies or suspicious activity.

Those are just a few examples

- Some Notable items:
  - Of 108 NIST CSF subcategories…only 12 lack a PCI-DSS analog
  - EVERY Requirement section in PCI-DSS has analogs in NIST-CSF
  - EVERY function (ID, PR, DE, RS, RC) in NIST-CSF has analogs in PCI-DSS. Only ONE category (RC.CO) does not.
- NIST items without a PCI analog tend to be in the 'A' leg of the triad (e.g., capacity planning), or relate to PR/Comm (e.g., after an IR)

Case Study: How it began

- A startup came to Sedara wanting guidance
- Their stated goal: “Get PCI-certified”
- They facilitate CC payments but have no CDE
- We started delving into their ISMS
  - They had no SDLC
  - They had no organizational policies
  - Their infra monitoring was just getting started
  - …but it only covered their on-prem, though the applications live in the cloud

Case Study: How it’s going

- They are now:
  - Building out a proper SDLC and institutionalizing it with their devops partner
  - Building segregated Dev, Test and Prod environments
  - Building out a proper data center, 100% monitored
  - Expanding monitoring to include their cloud footprint
  - Creating a body of policies and standards

- All these things are implicit in NIST CSF compliance, without even cracking the PCI-DSS book.

So what have we learned?

- NIST-CSF and PCI-DSS are both concerned with information security
- It's possible to correlate and coordinate the two frameworks
- A program that advances one advances the other
- Good infosec practices serve both safety AND compliance

Thank You

DAVID FRIER, CISM, CISSP, ETC.

$FIRST.$LAST @ { SEDARASECURITY | ROCINFOSEC } .COM