PrivacyOC

SoCal's Premier Data Privacy Event

The Interplay of Privacy, Security and Governance

It's a Matter of Trust

Neil R Packard, CISA/CIPM

Chief Security Consultant, SoCal Privacy Consultants

Today's Roadmap

- Distinguishing Information Privacy & Security
- Standards & Controls for Compliance
- Governance for Sustainability & Defensibility
  - Data Mapping
  - Risk Management
  - Journey to Maturity

Myths

Security is IT’s job

Privacy is Legal’s job

Data Protection is Privacy

Data privacy is a passing trend

We achieve compliance, we’re all done

Information Privacy & Security

Program Principles

SoCal Privacy Consultants

Operationalizing Privacy and Security Programs


privacy
information
personal
protection
internet
data
people
identity
government
law
rights
right
policy
individuals
secret
social
private
online
public
human
act
use
legal
sites
control
protect
location
technologies
freedom
invasion
market
countries
disclosure

$\neq$


INFORMATION
SECURITY
TECHNOLOGY
WORKSTATION
DATA
EMAIL
BUSINESS
ACCESS
PROJECT
DESIGN
COMPUTING
MOBILITY
SYSTEM
PRODUCTS
CLIENT
INFORMATION
VIRTUAL
OPERATION
CONTROL
KNOWLEDGE
PRODUCTS
PLANNING
MANAGER
INTERNET
LAPTOP
MOBILE
NETWORK
DATABASE
DESKTOP
PROCESS

Depends on your Point of View

Privacy	Security
Individual (Consumer) focused	Data focused, includes Bus. Confid.
Consumer rights & choices	Data protection
Notice/transparency (informed)	IP, network & asset protection
Legitimate purpose/consent for collection, use, access, sharing & retention (DPLC management)	Confidentiality, Integrity & Availability
***Authorized* access governance**	***Unauthorized access***
Laws, context, social norms/reasonable consumer expectations, principles & risk oriented	Standards & controls oriented
Includes security	Does not include privacy
Accountability / governance / trust	Often not included in standards

Privacy and Security

- Data Privacy Life Cycle
  - Notice
  - Consent/Choice
  - Rights
  - Use
  - Sharing
  - Retention
  - Disposal
- Governance

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Event vs. Incident vs. Breach

1. EVENT	2. INCIDENT
Policy: **Observable privacy / Infosec issue**, e.g., a **violation of policy**, must be reported to Privacy/Security Officials	**Policy**: **Attempted or successful unauthorized** access, use, disclosure, modification, or destruction of information **or interference with system operations** in an information system

3. *REPORTABLE* BREACH

California -

1. Requires a business or state agency to notify any California resident whose unencrypted **personal information** was compromised by an unauthorized person.
   - >500 California residents must notify California Attorney General
2. CMIA: Unauthorized access, use or disclosure of PHI [Confidentiality of Medical Information Act]

HIPAA: Acquisition, access, use, or disclosure of unsecured PHI not permitted by Privacy Rule which compromises security or privacy of PHI – based on 4 risk factors

Information Security

- Information security protects **all information assets** an organization collects and maintains.
- Security Controls
  - Limits information access
  - Protects from **unauthorized** use and acquisition.
  - Provides the controls for protecting personal information.

Information Privacy

- Focuses on the **personal information (PI)** an organization collects and maintains.
- A broader definition of **personal information (PI)** is *"any information related to an identified or an identifiable individual."*
- Operationizing in a practical way your legal obligations

What's in a name?

- **Pseudonymized – reduces risk but still under CCPA/GDPR**
  - **Personally identifiable information (PII)** is any information about an individual … including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is [directly] linked or linkable to an individual, such as medical, educational, financial, and employment information. - NIST

- **De-identified – Not within the scope of CCPA/GDPR**
  - **Personal Information (PI)** any information that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably be linked (directly or indirectly) with a particular consumer or household." - CCPA
    - The Act specifies a variety of new data elements constituting PI including but not limited to:
      - identifiers such as any unique personal identifier or IP address; electronic network activity information, including, **browser histories**, search history, and any information regarding a consumer's interaction with a Web site, application or advertisement; audio, electronic, visual, thermal, and olfactory information; and **geolocation data**.
    - In addition, the Act specifies any "inferences drawn" from various data elements of PI *"to create a **profile** about a consumer reflecting the consumer's preference, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes"* constitutes PI.
  - **Personal data (PD)** any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person - GDPR

Privacy & Security Program

Involves Common Governance but Different Domains

Requires a Holistic Approach

Needs a Common Language

A **successful** privacy program **requires** the **support** of a security program.

Privacy Program

Establishes governance with **clear roles & responsibilities** creating a sustainable foundation based on Framework

Sustainable, Defensible and Trustworthy Privacy (& Security) Program

Risk management program requires risk owners who identify & acceptably mitigate foreseeable risks (& document same) to be defendable to regulator & plaintiff judge/jury, *based on COSO's ERM approach & methodology*

Privacy Program

- Data & resource mapping
- Governance structure
- PI sensitivity classification
  - drives strength of controls
- Risk management: P/SbD, periodic
- Sanctions & complaints
- External resource management
- Monitoring, auditing & oversight
- Incident & breach management & response

Privacy Practices

- Data privacy lifecycle controls
  - notice, data collection, use, sharing & retention controls
- Data subject rights & choices
  - data infrastructure & management
- Data minimization (avoid re-identification)
  - e.g. min. necessary, key coding, de-identification, pseudonymization
- Verification & authentication

Security Practices

- Administrative safeguards
  - e.g., RBAC design, authorization & periodic review
- Physical controls
  - e.g., review of facility's physical controls
- Technical controls
  - e.g. use of encryption
- Engineering controls
  - e.g. implementation of Privacy/Security-by-Design/SDLC

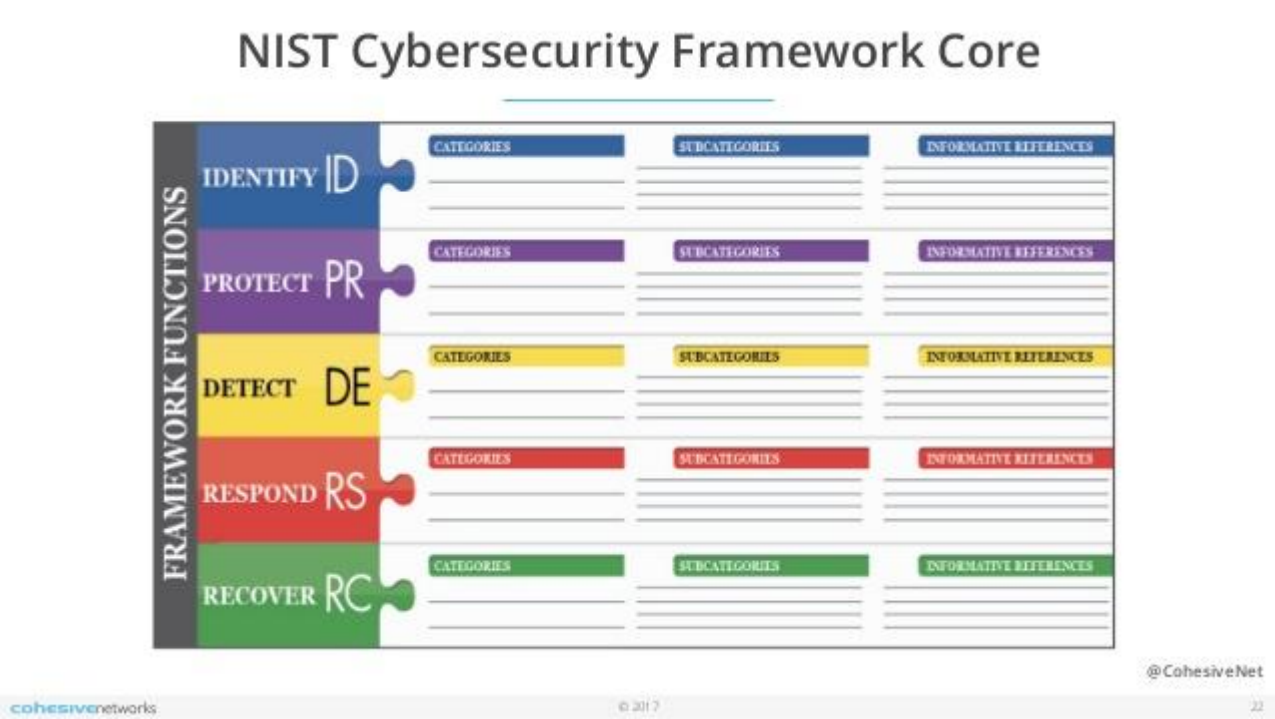
Compliance *establishes baseline*, however alone is ***not defensible*** as laws, regulations & standards cannot keep pace with emerging technologies – an effective risk management program closes this gap

Enterprise cross-functional collaboration & coordination

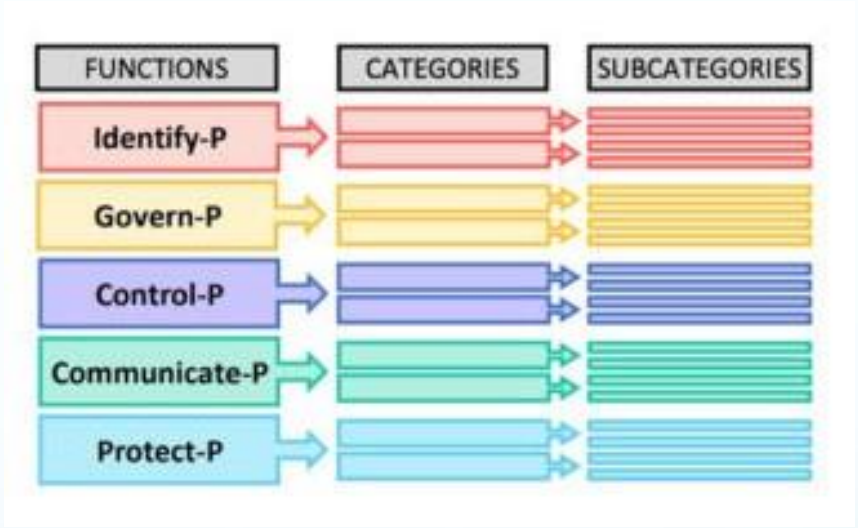
Common Frameworks

- NIST Cybersecurity Framework v1.1
- ISO/IEC 27000:2018 Information Security Management Systems
- Control Objectives for Information and Related Technology (COBIT)
- Generally Accepted Privacy Principles (GAPP) - AICPA/CICA
- NIST Privacy Framework v1.0

NIST Frameworks



NIST Privacy Framework



Generally Accepted Privacy Principles (GAPP)

SoCal Privacy Consultants
Operationalizing Privacy and Security Programs

No.	Principle Areas	Description	CCPA Sections	GDPR Articles	Criteria Total
1	**Management**	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.		5, 6, 14, 24, 27, 32, 36-39	**14**
2.1	*Policies and Communications*				3
2.2	*Procedures and Controls*				11
2	**Notice**	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.	1798.100(b) 1798.110 (c)	5,12-15, 21	**5**
2.1	*Policies and Communications*				2
2.2	*Procedures and Controls*				3
3	**Choice & Consent**	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.	1798.120 1798.120(d)	6, 7, 8	**7**
3.1	*Policies and Communications*				3
3.2	*Procedures and Controls*				4
4	**Collection**	The entity collects personal information only for the purposes identified in the notice.	1798.100(b)	5, 6, 9, 21, 25, 35, 89	**7**
4.1	*Policies and Communications*				3
4.2	*Procedures and Controls*				4
5	**Use - Retention - Disposal**	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.	1798.100(b)	5, 6, 10, 22, 39	**5**
5.1	*Policies and Communications*				2
5.2	*Procedures and Controls*				3
6	**Access**	The entity provides individuals with access to their personal information for review and update.	1798.100(a) 1798.110(a)(1)-(5)+ (b) 1798.130(a)(1)-(7)	7, 12, 14-18, 20-22, 26, 38	**8**
6.1	*Policies and Communications*				2
6.2	*Procedures and Controls*				6
7	**Third Party Disclosure**	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.	1798.140(v)+ (w) 1798.145(h)	28, 29, 32	**7**
7.1	*Policies and Communications*				3
7.2	*Procedures and Controls*				4
8	**Security for Privacy**	The entity protects personal information against unauthorized access (both physical and logical).	1798.81.5(b) 1798.150(a)(1)	5 ,6, 24, 32, 46	**9**
8.1	*Policies and Communications*				2
8.2	*Procedures and Controls*				7
9	**Quality**	The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.		5, 16	**4**
9.1	*Policies and Communications*				2
9.2	*Procedures and Controls*				2
10	**Monitoring & Enforcement**	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.		17, 19, 20, 30, 33-35, 37,39, 47	**7**
10.1	*Policies and Communications*				2
10.2	*Procedures and Controls*				5

Standards and Controls

A Dynamic Environment

SoCal Privacy Consultants

Operationalizing Privacy and Security Programs

What applies to me?

CALIFORNIA CONSUMER PRIVACY ACT (CaCPA)

Common Standards & Controls

Privacy

- EU's General Data Protection Regulation (GDPR)
- ISO/IEC 27701:2019 — Extension to ISO/IEC 27001/27002 for Privacy Information Management
- HIPAA/HITECH Privacy & Breach Notification Rules
- CA Consumer Privacy Act of 2018 (CCPA)
- Nevada + 48 states Privacy laws ???
- NIST Privacy Controls 800-53 r4 Appendix J
  - Rev5 + two families and integrates with Rev4 security controls
- Federal Privacy Law ???

Security

- Top 20 Critical Security Controls
- ISO/IEC 27002:2013
- HIPAA/HITECH Security Rule
- Payment Card Industry (PCI) Security Standards
- NIST Security Controls (800-53, 800-171)
- ISO/IEC 27001:2013 Information Security Management Systems

GDPR Combination

Privacy

- **EU's General Data Protection Regulation (GDPR)**
- **ISO/IEC 27701:2019 — Extension to ISO/IEC 27001/27002 for Privacy Information Management**
- HIPAA/HITECH Privacy & Breach Notification Rules
- CA Consumer Privacy Act of 2018
- Nevada + 48 states Privacy laws
- NIST Privacy Controls 800-53 r4 Appendix J
  - Rev5 + two families and integrates with Rev4 security controls
- Federal Privacy Law ???

Security

- **Top 20 Critical Security Controls**
- **ISO/IEC 27002:2013**
- HIPAA/HITECH Security Rule
- Payment Card Industry (PCI) Security Standards
- NIST System Controls (800-53, 800-171)

CCPA Combination **Minimum**

Privacy

- EU's General Data Protection Regulation (GDPR)
- ISO/IEC 27701:2019 — Extension to ISO/IEC 27001/27002 for Privacy Information Management
- HIPAA/HITECH Privacy & Breach Notification Rules
- **CA Consumer Privacy Act of 2018**
- Nevada + 48 states Privacy laws
- NIST Privacy Controls 800-53 r4 Appendix J
  - Rev5 + two families and integrates with Rev4 security controls
- Federal Privacy Law ???

Security

- **Top 20 Critical Security Controls**
- ISO/IEC 27002:2013
- HIPAA/HITECH Security Rule
- Payment Card Industry (PCI) Security Standards
- NIST System Controls (800-53, 800-171)

HIPAA Combination

Privacy

- EU's General Data Protection Regulation (GDPR)
- ISO/IEC 27701:2019 — Extension to ISO/IEC 27001/27002 for Privacy Information Management
- **HIPAA/HITECH Privacy & Breach Notification Rules**
- CA Consumer Privacy Act of 2018
- Nevada + 48 states Privacy laws
- NIST Privacy Controls 800-53 r4 Appendix J
  - Rev5 + two families and integrates with Rev4 security controls
- Federal Privacy Law ???

Security

- **Top 20 Critical Security Controls**
- ISO/IEC 27002:2013
- **HIPAA/HITECH Security Rule**
- Payment Card Industry (PCI) Security Standards
- NIST System Controls (800-53, 800-171)

Federal Contractor Combination

Privacy

- EU's General Data Protection Regulation (GDPR)
- ISO/IEC 27701:2019 — Extension to ISO/IEC 27001/27002 for Privacy Information Management
- HIPAA/HITECH Privacy & Breach Notification Rules
- CA Consumer Privacy Act of 2018
- Nevada + 48 states Privacy laws
- **NIST Privacy Controls 800-53 r4 Appendix J**
  - Rev5 + two families and integrates with Rev4 security controls
- Federal Privacy Law ???

Security

- **Top 20 Critical Security Controls**
- ISO/IEC 27002:2013
- HIPAA/HITECH Security Rule
- Payment Card Industry (PCI) Security Standards
- **NIST System Controls** (800-53, **800-171**)

Mind the Gaps

Control	HIPAA	GDPR	CIS Top 20	ISO 27001	CCPA
Inventory	§164.310(d)(1) §164.310(d)(2)(iii)		CSC 1, 2	A.8.1.1 A.9.1.2 A.12.5.1 A.12.6.2 A.13.1.1	
Access	§164.308(a)(3)(i)	Articles 15 **(Rights)** 32 (Security)	CSC 9 CSC 12 CSC 15 CSC17	A.7.2.2, A.9.1.2 A.10.1.1, A.12.4.1 A.12.7.1, A.13.1.1 A.13.1.3, A.13.2.1 A.13.2.2, A.13.2.3 A.14.1.2	1798.150 (Security) 1798.100.d **(Rights)**
Responsibility	§164.308(a)(2)	Article 24, 26, 39		A.6.1.1	
Authorization	§164.308(a)(3)(ii)(A)		CSC 14, 16		1798.120

Information Governance

SoCal Privacy Consultants

Operationalizing Privacy and Security Programs

What is Information Governance?

- A system of **policies & processes** where information (data) life cycle activities are directed, controlled, & monitored; and assure sustainability & reliability
  - NIST “Repeatable” state
- How do you direct, control & monitor?
  - Clear roles & responsibilities defined in policies & training
    - Too many P&Ps state “*we*” or “*company*” does this or that …

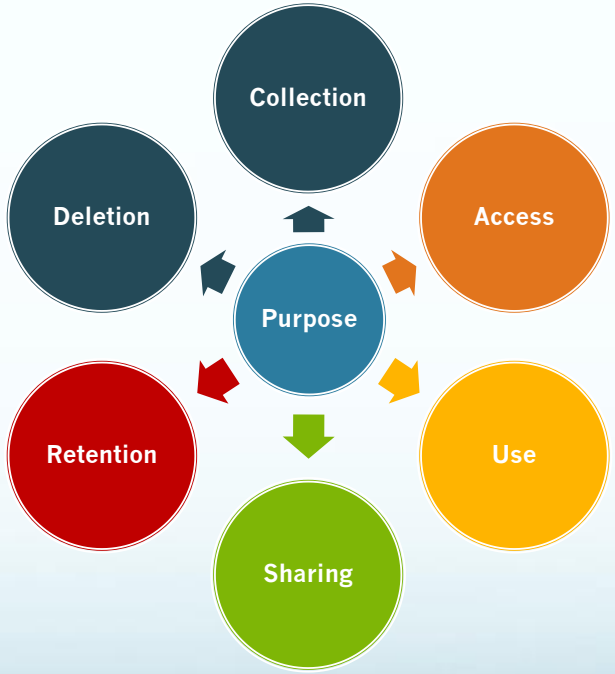
Foundational Program Governance

#	Privacy	Security
1	Organizational Governance	Same
2	Governance via Policy	Same
3	HR Governance: pre-onboarding, onboarding, employed & termination	Same
4	Data Privacy Life Cycle & Resource Governance	Data & Resource Mapping portion
5	Privacy Rights Governance	N/A
6	Privacy-by-Design Governance	Security-by-Design Governance
7	Same	External Resource Mgmt Governance
8	Monitoring & Evaluation/Auditing Governance	Same
9	Event & Incident Management Governance	Same
10	Documentary Evidence of Governance	Same
11	Program KPIs & Governance Reporting	Same

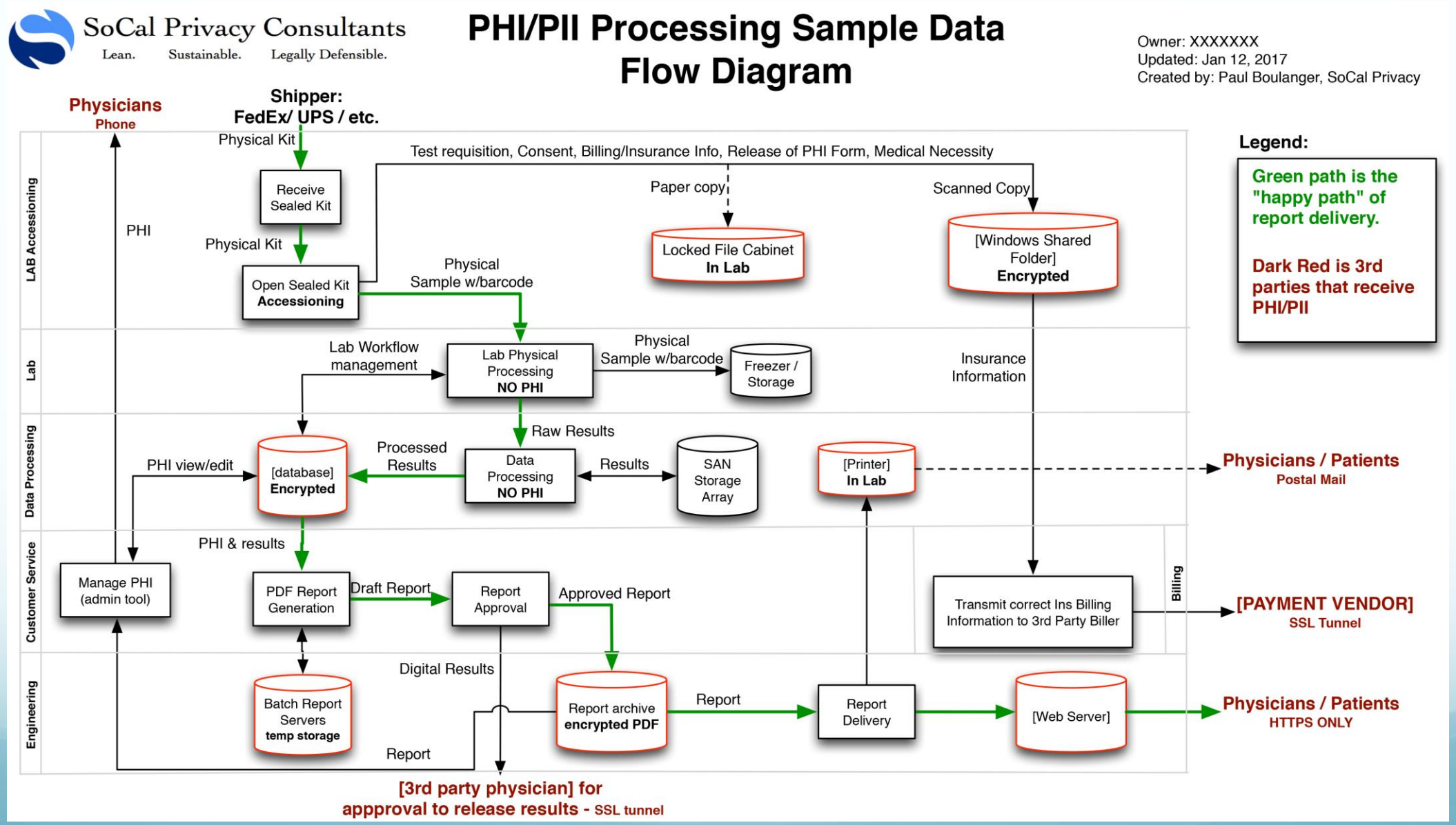
External Resource Management means governance of **service providers & 3rd parties** under CCPA

Data Privacy Life Cycle & Resource Governance

- Data Map
  - Inventory/document all DPLC sub-processes
- Validate/record legitimate/business purpose for all DPLC sub-processes in risk register
  - Data collection
  - Data access
  - Data use
  - Data sharing
  - Data retention
  - X-border data transfers
- Stop non-compliant processes
- Remove non-compliant data



Data Mapping



Data sensitivity drives a risk-based approach

Determine strength of controls based on data sensitivity levels

Quartile	Data Sensitivity Classifications	Examples
4	**Highly Sensitive**	1st name/initial & last name plus any of following: gov't issued ID # (SSN, passport ID#, state ID#, driver's license#, tax ID#, birth/marriage certificate), W-2, health insurance ID#, genetic info (defined by GINA), medical/health info (medical history, physical/mental condition, test results, diagnosis, treatment/medications), background check info, biometric data/record or identifiers, digital signature, precise geo-location data, username/ID or email address w/password or common security question answers (mother's maiden name, DOB, place of birth), financial acct # or payment card info plus any required security/access code or password
3	**Sensitive**	PI that does not fall into highly or less sensitive PII groups, such as other personally identifiable dates, vehicle ID/serial #, other unique ID#/characteristic/code, non-precise geo-location data, other personnel file info
2	**Slightly Sensitive**	Published contact info: name plus address, phone#; email address, fax#, instant message user ID, URL address, IP address, photo/video/audio file, persistent device/processor/serial ID; any other PII used for marketing purposes (see CA's "Shine the Light Law")
1	**Non-Sensitive**	non-personal information, such as session identifiers/cookies

Risk Management

- Framework
  - Identify events
  - Assess events
    - Determine event impacts
  - Develop strategy to respond
  - Monitor progress

Risk Management Goal

Management Making informed decisions

- Develop Strategic Plan
- Improve organization's capability and coordination to effectively manage risk
- Integrate and present a unified picture of risk to the stakeholders
- Demonstrate making informed decisions

Challenges

- Implementing Risk Management is a formidable task
  - Designing an **appropriate** model
  - Obtaining top management **participation**
  - Assure **meeting** organizational objectives
  - Moving in a **coordinated and comprehensive** approach

Risk Ownership

- **Executives** should assign owners to resources w/in organizational control (or by default become owner for such resources) & inform PO/SO, so resources & owners can be recorded in resource map
- **Risk owners** own risks inherent in their people, process & technology
  - Identified in data flow, inventory & resource/locations mapping
- **Product/project managers** in collaboration with engineering are primarily responsible for Privacy & Security-by-Design of resources

Resources

- **Resources**:
  - Products/services, processes, apps/software, databases, internal/external systems
    External resources: service providers, 3rd parties, supply chain
- **Resource Owners** are responsible for ensuring RBAC design, authorizing RBAC rights, & periodically reviewing RBAC rights for accuracy
- **Resource Custodians** are responsible for implementing authorized RBAC rights & providing reports of all rights for periodic review by resource owner
  - Works with DSAR Coordinator to fulfill consumer rights

COSO Internal Control — Integrated Framework

Internal Control Objectives

Control Components

Organization Hierarchy

Path to Maturity

Mature State: P/SbD

Resilient
Trustworthy
Defensible

Action Plan: Crawl, Walk, Run

Control Gaps
Risks

Foundation

Policies & Procedures
Governance – Accountability – Responsibility
Establishing Repeatable Processes

GRC "*Check-the-box*" Approach

Requirements	Compliant	Non-compliant
P/SbD	✓	
Periodic Risk Assessment	✓	
Vendor Risk Assessment	✓	
Segregation of Duties		✓
Continuous Monitoring	✓	

Is this a sufficient evaluation methodology?

Program Practices & Maturity

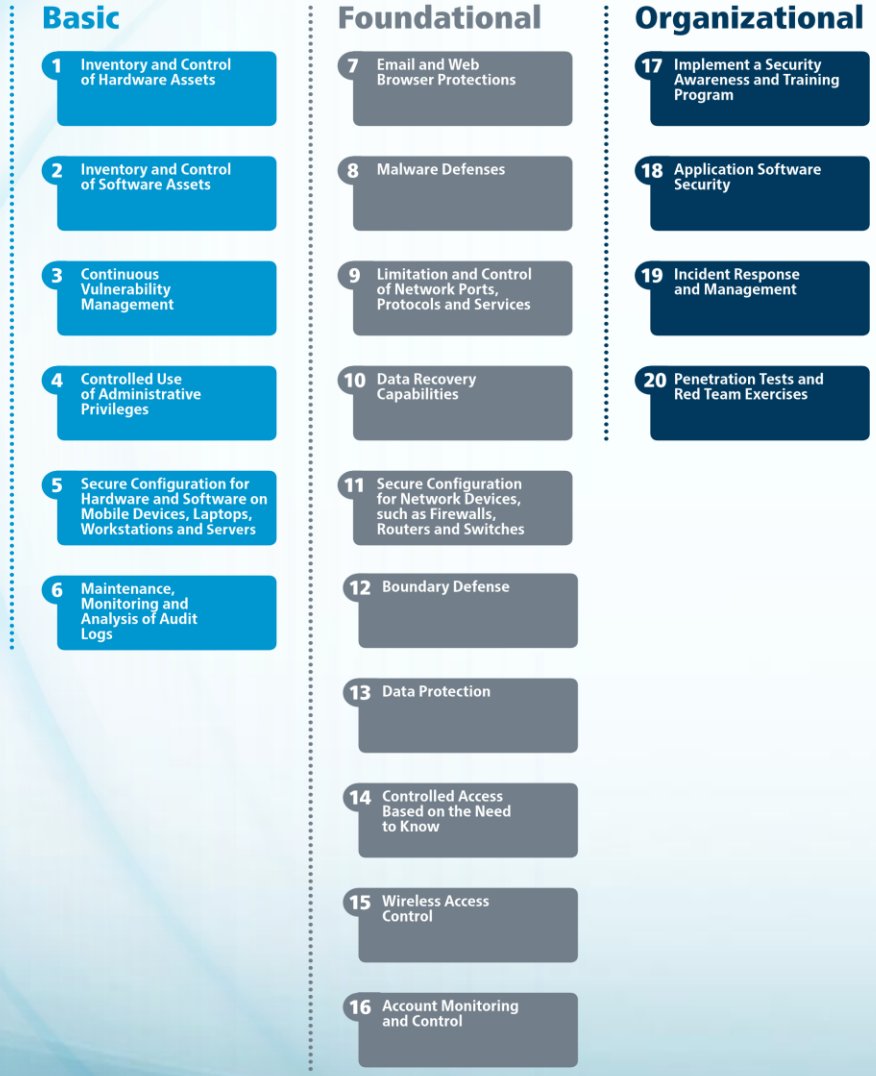
	Level 1	Level 2	Level 3	Level 4	Level 5
Practices	Demonstrate basic cybersecurity & privacy hygiene	Demonstrate intermediate cybersecurity & privacy hygiene	Demonstrate good cybersecurity & privacy hygiene	Demonstrate substantial cybersecurity & privacy programs	Demonstrate optimized capabilities addressing dynamic events
Maturity	Nothing · Adhoc	Established policies, SOPs, & plans	Activities reviewed for adherence to policy & procedures	Activities reviewed for effectiveness and management is informed of any issues	Activities are standardized across all applicable organizational units and identified improvements are shared

Based on the DOD Cybersecurity Maturity Model Certification (CMMC) v0.7 *Draft*

NIST Risk Management ("RM") Implementation Tiers

Tier	Risk Level	Risk Management Process	Integrated RM Program	External Actions
1	**PARTIAL**	Informal, ad-hoc, reactive	Limited awareness	No processes in place
2	**RISK INFORMED**	Management approved RM practices are not established policy	Risk awareness but informal RM	Awareness, but not formalized
3	**REPEATABLE**	Sustainable, Formal RM practices in policy	Formal policies/ procedures are implemented/ reviewed	Understand dependencies collaborate with other entities
4	**ADAPTIVE**	Lessons learned & predictive indicators inform RM practices	RM is part of the culture	Collaboration ensures accurate, current information shared

Controls Maturity Example



CIS Top 20

171 Sub-controls

Implementation Groups

Group 1 – 43 Controls

Limited resources/expertise
Low sensitivity

Group 2 – 99 Controls

Moderate resources/expertise
Sensitive

Group 3 – 29 Controls

Significant resources/expertise
Reduce impact of zero-day/targeted attacks

Monitoring & Evaluation

Governance Operational Recommendations

- Establish, in policy, mechanisms for periodic evaluations/ monitoring, reporting of findings & overseeing appropriate implementation of corrective actions/mitigation plans
- **Define activities in policy, assign ownership & timetables**
  - Regular, appropriate patching - FTC emphasis
  - Periodic risk assessment & controls evaluation
  - Periodic vulnerability scans & penetration tests
  - Periodic code reviews
  - Periodic RBAC rights review
  - Periodic hardware/software inventory reconciliation
  - Periodic review of access points & wireless
  - Periodic external resource due diligence based on data sensitivity
  - Periodic incident response desktop exercise &/or simulation
  - Periodic testing of Business Continuity & Disaster Recovery plans

Additional Resources

- **CISO Desk Reference Guide: A Practical Guide for CISOs** by Bill Bonney, Gary Hayslip, Matt Stamper
  https://www.amazon.com/CISO-Desk-Reference-Guide-Practical/dp/0997744111
- **Kill Chain**
  https://www.csoonline.com/article/2134037/cyber-attacks-espionage/strategic-planning-erm-the-practicality-of-the-cyber-kill-chain-approach-to-security.html
- **OWASP Top 10** Most Critical Web Application Security Risks
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- **Application Security Guide for CISOs**
  https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs
- Cloud Security Alliance's **Cloud Security Controls Matrix**
  https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview
- **Shared Responsibility Models**
  https://aws.amazon.com/compliance/shared-responsibility-model/
  https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Additional Resources

- **The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value**
  https://www.amazon.com/Privacy-Engineers-Manifesto-Getting-Policy-ebook/
- **Generally Accepted Privacy Principles**
  https://iapp.org/media/presentations/11Summit/DeathofSASHO2.pdf
- **NIST Privacy Framework**
  https://www.nist.gov/privacy-framework
- **California Consumer Privacy Act**
  https://www.oag.ca.gov/privacy/ccpa
- **General Data Protection Regulation (GDPR)**
  https://gdpr-info.eu/
- **International Association of Privacy Professionals**
  https://www.iapp.org

Questions?

Privacy	Security
Individual (Consumer) focused	Data focused, includes Bus. Confid.
Consumer rights & choices	Data protection
Notice/transparency (informed)	IP, network & asset protection
Legitimate purpose/consent for collection, use, access, sharing & retention (DPLC management)	Confidentiality, Integrity & Availability
***Authorized* access governance**	***Unauthorized access***
Laws, context, social norms/reasonable consumer expectations, principles & risk oriented	Standards & controls oriented
Includes security	Does not include privacy
Accountability / governance / trust	Often not included in standards

Neil R Packard, CISA/CIPM

npackard@socalprivacy.com

619.208.2529

www.socalprivacy.com

SoCal Privacy Consultants

Operationalizing Privacy and Security Programs

PrivacyOC

SoCal's Premier Data Privacy Event

THANK YOU!

Platinum Sponsor

privageo

Data Privacy... Solved.

Active Navigation

BigID

INTEGRIS SOFTWARE

OneTrust

PRIVACY, SECURITY & THIRD-PARTY RISK

Procopio

Severson & Werson

A Professional Corporation

BakerHostetler

CENTRL

Klinedinst ATTORNEYS

PRIVACI.ai

RUTAN

RUTAN & TUCKER, LLP

truyo