

Business Case

- Mitigate company regulatory, legal, financial and reputation risks, and loss of productivity due to a breach.
- Protect customers and employees from financial, medical, and reputation risks associated with identity theft.
- Protect company intellectual property and trade secrets and infrastructure and technology from compromise and business disruption.
- Enable business development, M&A and investment opportunities.
- Protect executives and directors from D&O class action lawsuits and job loss.

Presumption of a Breach

Regulators advise, organizations must presume they will inevitably suffer a data breach. Unfortunately, compromised organizations learn the hard way, **check-the-box compliance does not establish a legally defensible posture**. This means, in addition to the direct costs of a breach, organizations are exposed to additional legal costs, regulatory fines, and burdening oversight, such as a 20 year FTC consent order.

Organizations need to systematically and continuously identify and document foreseeable risks, apply reasonable standards of care, and defend risk-based decisions to an oversight authority, plaintiff attorney, judge, or jury.

Value Proposition

SoCal Privacy helps public and private organizations establish a lean, sustainable, legally defensible security and privacy program, including appropriate data governance with clear roles and responsibilities. We work with you to develop data flow maps, inventories, and locations, and use these to help you identify foreseeable risks. These risks are assessed, controls evaluated for effectiveness, and, where appropriate, mitigation plans developed to improve the strength of controls. We categorize data into sensitivity levels using a risk management approach, and help you develop scalable strategies, policies and procedures that match the strength of controls to the data sensitivity level, such as for an enterprise cloud use case strategy. As another example, service provider requirements for due diligence, agreement's reps and warranties, and periodic monitoring will be based on data sensitivity levels.

Contact Us

SoCal Privacy Consultants
35523 Royal Court
Winchester, CA 92596-8966

Phone: 619-318-1263

info@socalprivacy.com

www.socalprivacy.com



SoCal Privacy Consultants

Lean. Sustainable. Legally Defensible.

SoCal Privacy Consultants



Who We Are

Lean

We develop strategies to right-size our clients' privacy and security programs based on organizational size, complexity, objectives, risk profile, and risk tolerance.

Sustainable

We help clients establish effective and scalable governance with clear roles and responsibilities to continually sustain their organization's privacy and security program.

Legally Defensible

We help clients develop and implement a risk management approach to identify foreseeable risks and apply reasonable standards of care to create a legally defensible posture.

Services

Privacy and Security Gap Assessment

- For companies, subsidiaries, M&A buyers / sellers
- Policies and procedures review
- Data flow, inventory and locations mapping
- Controls evaluation to standards
- Risk assessment
- Findings and recommendations report
- Effective knowledge transfer

Privacy and Security Program Establishment

- Design governance infrastructure and roles and responsibilities and assist in kicking off program
- Define risk management and controls framework
- Develop policies and procedures
- Develop and deliver training
- Design program monitoring
- Obtain executive and board commitment

Third Party Due Diligence and Management

- Pre-contract due diligence and contract requirements
- Cloud services (use cases) policy and guidance
- Managed security services – build vs. buy guidance
- Provide third party management policy around due diligence, contracting, and ongoing monitoring

Privacy-by-Design (including Security)

- Privacy Impact Assessments during product design to inform privacy notice, requirements, and controls
- Privacy engineering (SDLC) policy and training for project managers and developers
- E.g. big data, mobile apps, IoT, websites, health care applications: where Personal Information is collected

Support Hiring and Development

- Source and interview CPO / CISO candidates
- Train and mentor internal candidates

Visit us at:
www.socalprivacy.com

More Services

Expert Privacy Consulting Services (on retainer or per project)

- Build and / or maintain Privacy Notice
- Privacy-by-Design guidance
- Data flow, inventory and locations mapping
- Comprehensive controls evaluation
- Risk assessment
- Develop policies and procedures
- Deliver user, developer, and management training
- Cross border transfer rules guidance
- Support business development by helping respond to third party due diligence requests
- Conduct due diligence on third parties
- Audit preparation

Standards and Controls We May Use to Assess Your Privacy and Security Posture

- ▶ CIS Top 20 Critical Security Controls
- ▶ HIPAA / HITECH
- ▶ GDPR
- ▶ CA Consumer Privacy Act of 2018
- ▶ NIST Cybersecurity Framework
- ▶ ISO/IEC 27002:2013
- ▶ SEC OCIE Cybersecurity Initiative
- ▶ GAPP (Generally Accepted Privacy Principles)
- ▶ U.S. Sentencing Guidelines for Effective Compliance Programs



SoCal Privacy Consultants

Lean. Sustainable. Legally Defensible.

Certifications

Certified Information
Privacy Professional
CIPP



Certified Information
Systems Auditor
CISA



Affiliations

International
Association of
Privacy Professionals
IAPP



Information Systems
Audit and Control
Association
ISACA



Association for
Information and Image
Management
AIIM



InfraGard

