OPTIMIZE IT COMPLIANCE PROCESSES TO MEET NEW DATA PRIVACY CHALLENGES

Ralph Villanueva CISA CISM PCI-ISA PCIP ITIL CIA CRMA CFE
IT Security and Compliance Analyst
Diamond Resorts

SCCE™
Society of Corporate Compliance and Ethics

1

Key takeaways

- The audience will learn the common data privacy requirements across several legislations such as the GDPR and the California Privacy Act, and understand the interrelatedness of IT compliance and data privacy
- The speaker will demonstrate how IT compliance processes can be leveraged to meet data privacy requirements
- Audience will pick up techniques to make their organizations more data privacy compliant upon returning to the office

SCCE™
Society of Corporate Compliance and Ethics

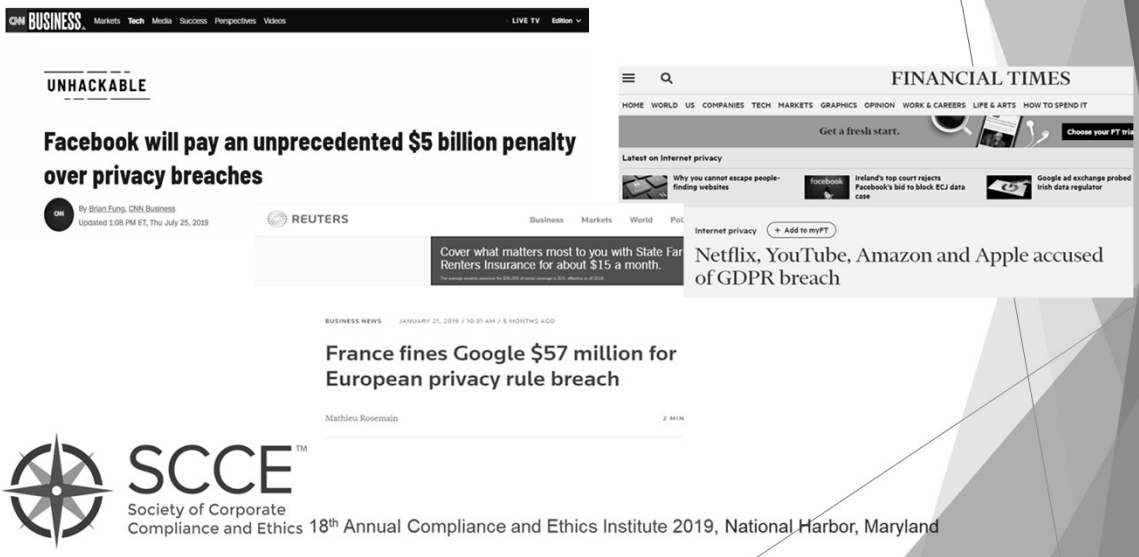
2

About Ralph Villanueva

- Relevant IT certifications such as CISA, CISM, ITIL Foundation v3, PCI-ISA and PCIP
- Relevant audit certifications such as CIA, CRMA and CFE
- Combined IT compliance and audit work experience of almost 20 years
- Believes that YOU can make a difference in meeting data privacy challenges

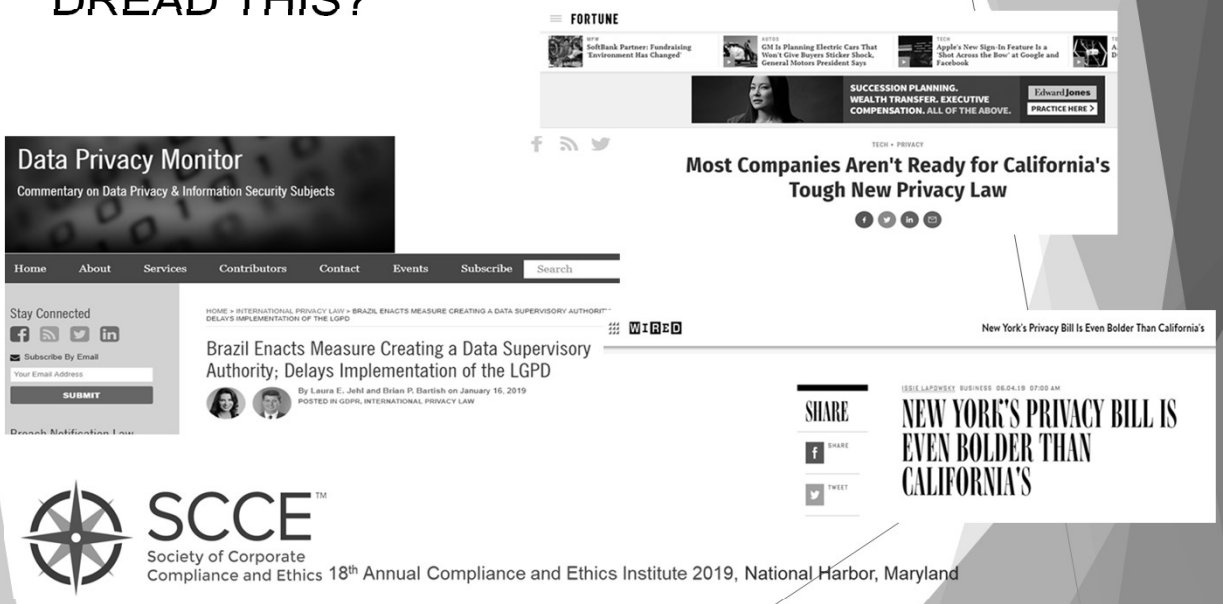
3

READ THIS?



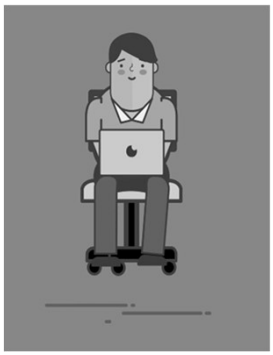
4

DREAD THIS?



5

EXPERIENCED THIS?

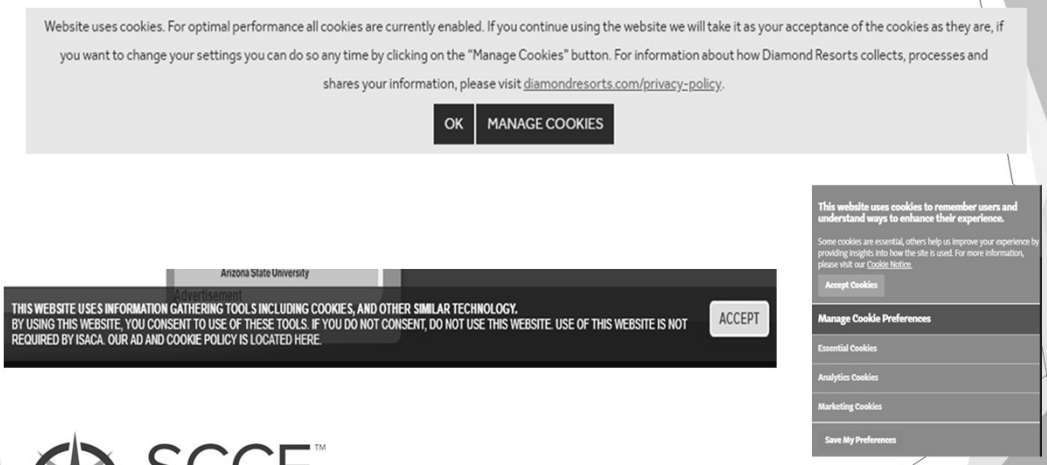


Last week

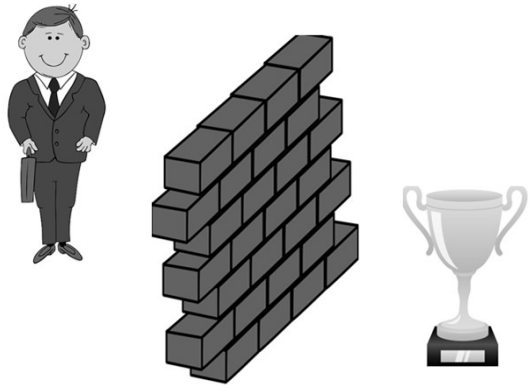
Today

6

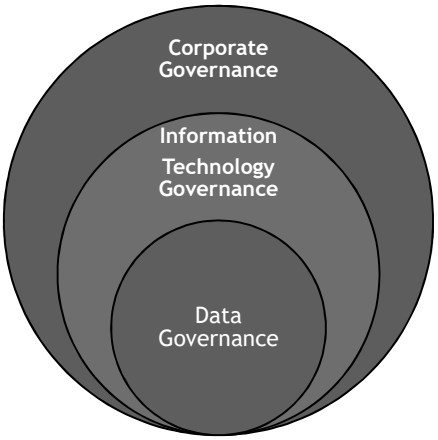
ENCOUNTERED THIS?



How do you get to the data privacy prize?

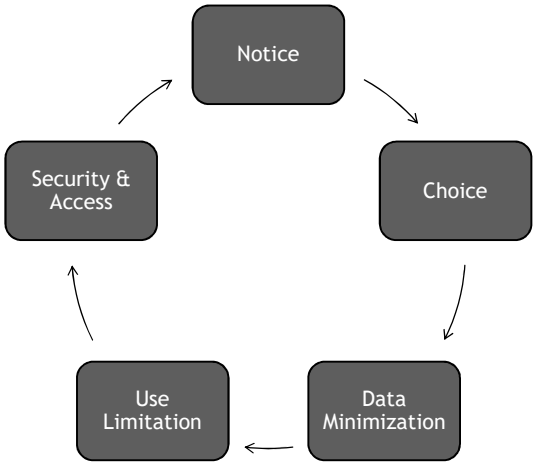


Understand place of data governance and privacy



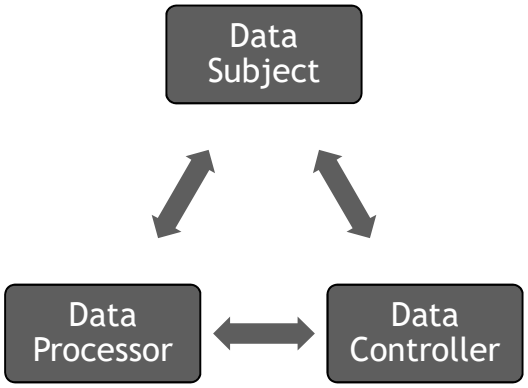
9

Know the data privacy principles



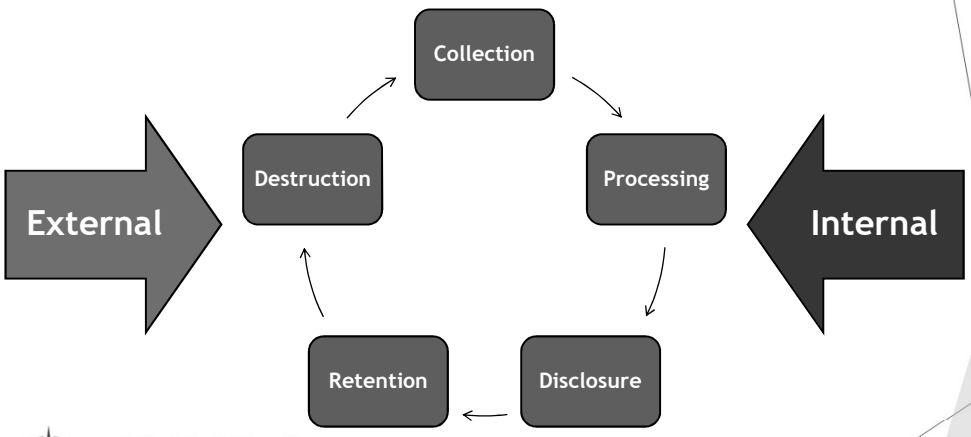
10

Know the data privacy players



11

Appreciate the data privacy environment



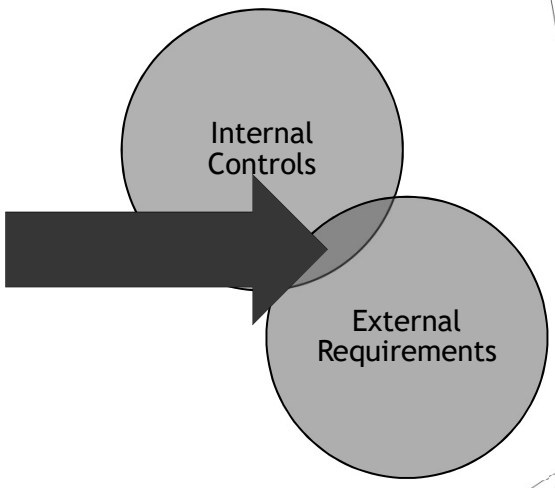
12

Overlap of controls and privacy requirements

13

Overlap of controls and privacy requirements

Segregation of duties
Authentication measures
Least privilege access control



14

Overlap of controls and privacy requirements

PCI DSS Requirements	Testing Procedures
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**12.4.a** Verify that information security policies clearly define information security responsibilities for all personnel.
	12.4.b Interview a sample of responsible personnel to verify they understand the security policies.

PCI DSS Requirements	Testing Procedures
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	**7.1** Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: • Defining access needs and privilege assignments for each role • Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities • Assignment of access based on individual personnel's job classification and function • Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.

Overlap of controls and privacy requirements

A.6 Organization of information security		
A.6.1 Internal organization		
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas ofresponsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

A.9 Access control		
A.9.4 System and application access control		
Objective: *To* prevent unauthorized access to systems and applications.		
A.9.4.1	Information access restriction	*Control* Access to information and application system functions shall be restricted in accordance with the access control policy.
A.9.4.2	Secure log-on procedures	*Control* Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

Overlap of controls and privacy requirements

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

17

Overlap of controls and privacy requirements

TITLE 1.81.5. CALIFORNIA CONSUMER PRIVACY ACT OF 2018

1798.100. (a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred

18

Overlap of controls and privacy requirements

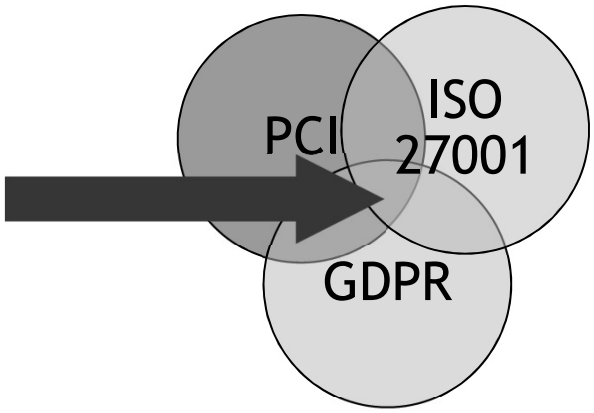
NRS 603A.210 Security measures.

1. A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

2. A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

Overlap of controls and privacy requirements

Internal Controls
- People
- Process
- Technology



Overlap of controls and privacy requirements

IC	PCI-DSS	GDPR
• Access control - user access be commensurate to job functions and responsibilities	• Req#07 -Restrict access to cardholder data by business need to know	• Article 5.1 (f) Processed in a manner that ensures appropriate security……including protection against unauthorized or unlawful processing

Overlap of controls and privacy requirements

IC	PCI-DSS	GDPR
• Information security policy – set of policies that ensures protection of organizational information	• Req#12 – Maintain a policy that addresses information security for all personnel	• Article 28.3 (b) – ensures that persons authorized to process personal data have committed themselves to confidentiality…

Overlap of controls and privacy requirements

IC	ISO 27001	CCPA
• Identify and document compliance with regulatory and contractual requirements	• A.18.1.1 – Identification of applicable legislation and contractual requirements	• 1798.100 (a) – A consumer shall have the right to request that a business that collect's a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

Overlap of controls and privacy requirements

IC	ISO 27001	CCPA
• Customer data protection policies	• A.18.1.4 – Privacy and protection of personally identifiable information	• 1798.120 (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information.

Overlap of controls and privacy requirements

IC	ISO 27001	NRS
• Customer data protection policies	• A.18.1.4 – Privacy and protection of personally identifiable information	• NRS 603A.210 (1) A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records….

Leveraging IT compliance processes to meet data privacy requirements

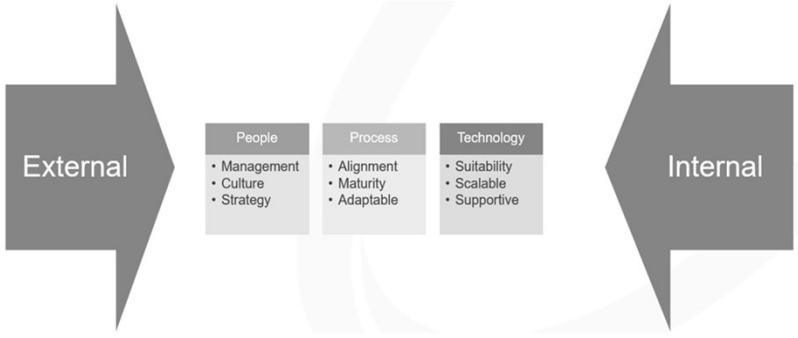
GDPR Article 32 - Security of Processing		Internal Controls, Policies and Measures	PCI-DSS References	ISO 27001 References
Article 32	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:	Annual Risk Assessment, Weekly CAB Meetings, IT Security Policies	PCI Req#12: Maintain a policy that addresses information security for all personnel	A.5.1.1: Policies for Information Security. A14.1: Security requirements of information systems
Article 32 , 1 (a)	the pseudonymisation and encryption of personal data	Tokenization of PII and CHD, IT Security Policies	PCI Req#03: Protect stored cardholder data. PCI Req#04: Encrypt transmission of cardholder data across open,	A.10.1 Cryptographic Controls
Article 32 , 1 (b)	the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	Tokenization of PII and CHD, IT Security Policies	PCI Req#07: Restrict access to cardholder data by business need to know.	A.9.4 System and application access control

Leveraging IT compliance processes to meet data privacy requirements

- Identify key privacy regulation provisions
- Classify those into people, process or technology requirement
- Look into your framework, policies and procedures
- Map those to the provisions
- Identify gaps and collaboratively work to bridge those

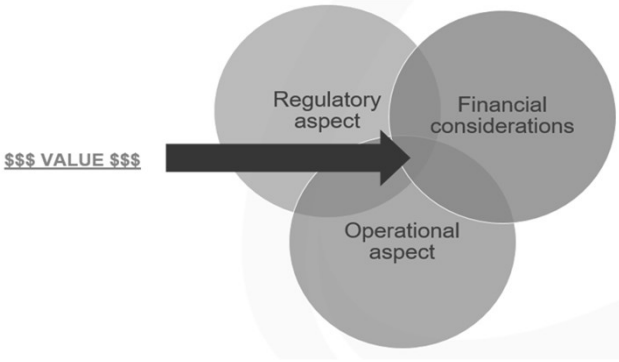
And here's some additional advice

Overcoming roadblocks to your compliance initiatives



And one more

The sweet spot in your compliance recommendations



Thank you very much