

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



SCCETM

Society of Corporate
Compliance and Ethics

18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

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



SCCETM

Society of Corporate
Compliance and Ethics

18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

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



SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

3

READ THIS?

CNN BUSINESS Markets Tech Media Success Perspectives Videos LIVE TV Edition

UNHACKABLE

Facebook will pay an unprecedented \$5 billion penalty over privacy breaches

By Brian Fung, CNN Business
Updated 1:08 PM ET, Thu July 25, 2019

REUTERS

Business Markets World Pol

Cover what matters most to you with State Farm Renters Insurance for about \$15 a month.

FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS GRAPHICS OPINION WORK & CAREERS LIFE & ARTS HOW TO SPEND IT

Get a fresh start.

Latest on Internet privacy

Why you cannot escape people-finding websites

Facebook

Ireland's top court rejects Facebook's bid to block ECJ data case

Google ad exchange probed with data regulator

Internet privacy + Add to myFT

Netflix, YouTube, Amazon and Apple accused of GDPR breach

BUSINESS NEWS JANUARY 21, 2019 / 10:31 AM / 5 MONTHS AGO

France fines Google \$57 million for European privacy rule breach

Mathieu Rosemain

2 MIN



SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

4

DREAD THIS?

Data Privacy Monitor
Commentary on Data Privacy & Information Security Subjects

Home About Services Contributors Contact Events Subscribe Search

Stay Connected



Subscribe By Email

Your Email Address

SUBMIT

Breakfast Modification 1 out

HOME » INTERNATIONAL PRIVACY LAW » BRAZIL ENACTS MEASURE CREATING A DATA SUPERVISORY AUTHORITY DELAYS IMPLEMENTATION OF THE LGPD

Brazil Enacts Measure Creating a Data Supervisory Authority; Delays Implementation of the LGPD



By Laura E. Jehl and Erian P. Barish on January 16, 2019
POSTED IN GDPR, INTERNATIONAL PRIVACY LAW



Most Companies Aren't Ready for California's Tough New Privacy Law



TECH » PRIVACY

SUCCESSION PLANNING, WEALTH TRANSFER, EXECUTIVE COMPENSATION. ALL OF THE ABOVE.

Edward Jones
PRACTICE HERE >

New York's Privacy Bill Is Even Bolder Than California's

SHARE

f SHARE

TWEET

ISSUE LATESTST BUSINESS 06:04:19 07:00 AM

NEW YORK'S PRIVACY BILL IS EVEN BOLDER THAN CALIFORNIA'S



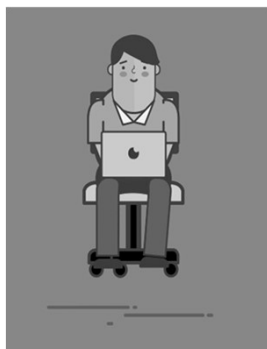
SCCETM

Society of Corporate

Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

5

EXPERIENCED THIS?



Last week



Today



SCCETM

Society of Corporate

Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

6

ENCOUNTERED THIS?

Website uses cookies. For optimal performance all cookies are currently enabled. If you continue using the website we will take it as your acceptance of the cookies as they are, if you want to change your settings you can do so any time by clicking on the "Manage Cookies" button. For information about how Diamond Resorts collects, processes and shares your information, please visit diamondresorts.com/privacy-policy.

OK

MANAGE COOKIES

Arizona State University
Advertisement
THIS WEBSITE USES INFORMATION GATHERING TOOLS INCLUDING COOKIES, AND OTHER SIMILAR TECHNOLOGY. BY USING THIS WEBSITE, YOU CONSENT TO USE OF THESE TOOLS. IF YOU DO NOT CONSENT, DO NOT USE THIS WEBSITE. USE OF THIS WEBSITE IS NOT REQUIRED BY ISACA. OUR AD AND COOKIE POLICY IS LOCATED HERE.

ACCEPT

This website uses cookies to remember users and understand ways to enhance their experience.

Some cookies are essential, others help us improve your experience by providing insights into how the site is used. For more information, please visit our [Cookie Notice](#).

Accept Cookies

Manage Cookie Preferences

Essential Cookies

Analytics Cookies

Marketing Cookies

Save My Preferences

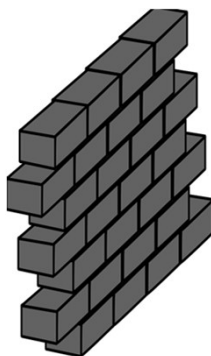


SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

7

How do you get to the data privacy prize?

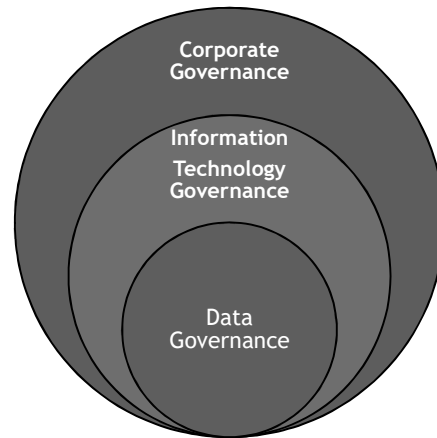


SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

8

Understand place of data governance and privacy

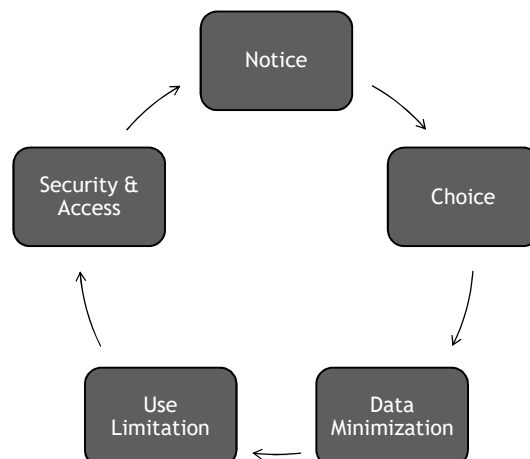


SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

9

Know the data privacy principles

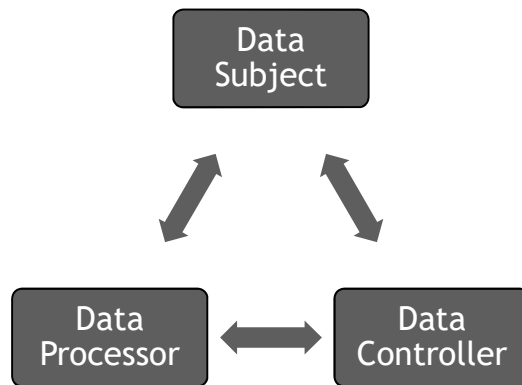


SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

10

Know the data privacy players

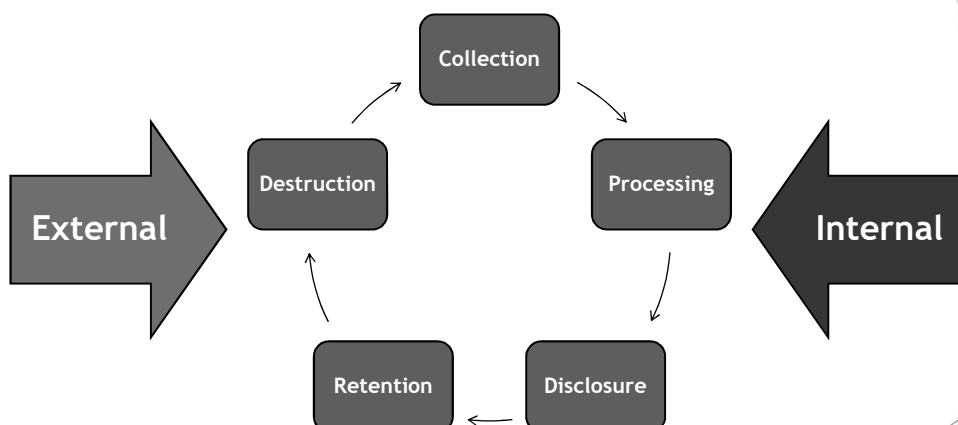


SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

11

Appreciate the data privacy environment

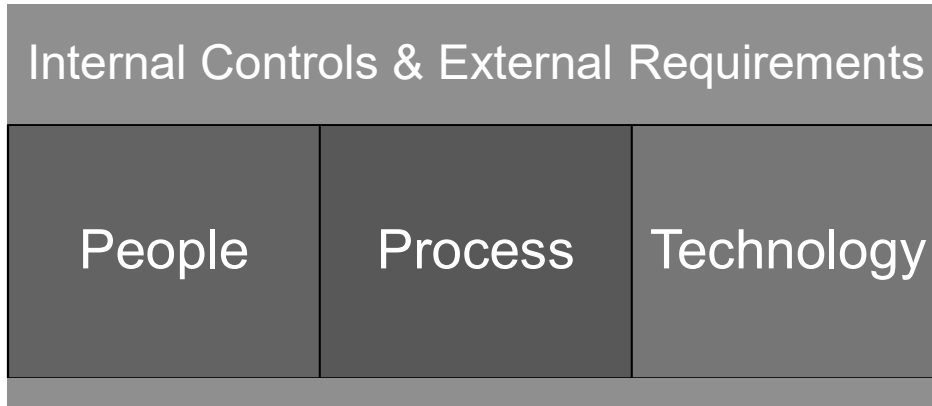


SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

12

Overlap of controls and privacy requirements

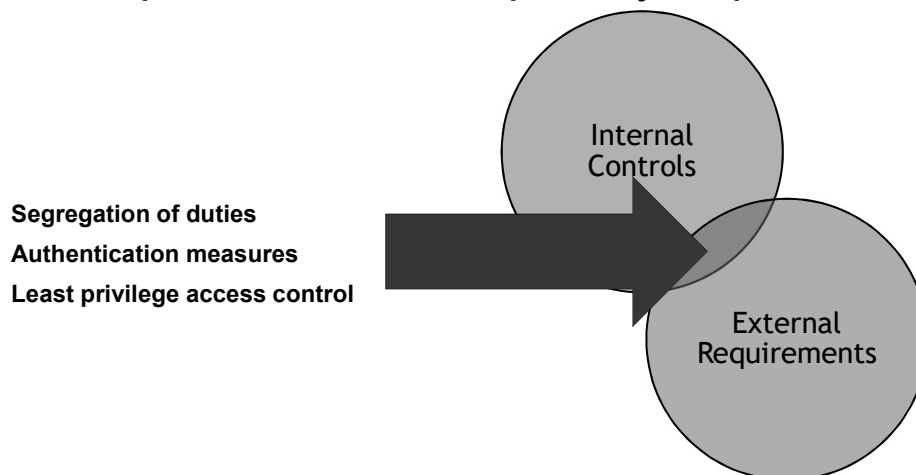


SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

13

Overlap of controls and privacy requirements



SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

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: <ul style="list-style-type: none"> 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.



SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

15

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 of responsibility 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.



SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

16

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:



SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

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



SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

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.



SCCETM

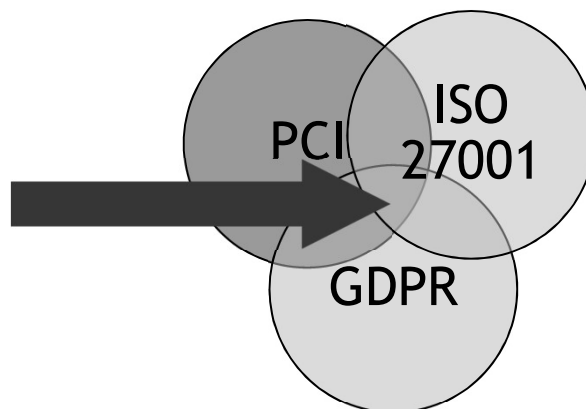
Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

19

Overlap of controls and privacy requirements

Internal Controls

- People
- Process
- Technology



SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

20

Overlap of controls and privacy requirements

IC

- Access control - user access be commensurate to job functions and responsibilities

PCI-DSS

- Req#07 -Restrict access to cardholder data by business need to know

GDPR

- Article 5.1 (f) Processed in a manner that ensures appropriate security.....including protection against unauthorized or unlawful processing



SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

21

Overlap of controls and privacy requirements

IC

- Information security policy – set of policies that ensures protection of organizational information

PCI-DSS

- Req#12 – Maintain a policy that addresses information security for all personnel

GDPR

- Article 28.3 (b) – ensures that persons authorized to process personal data have committed themselves to confidentiality...



SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

22

Overlap of controls and privacy requirements

IC

- Identify and document compliance with regulatory and contractual requirements

ISO 27001

- A.18.1.1 – Identification of applicable legislation and contractual requirements

CCPA

- 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.



SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

23

Overlap of controls and privacy requirements

IC

- Customer data protection policies

ISO 27001

- A.18.1.4 – Privacy and protection of personally identifiable information

CCPA

- 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.



SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

24

Overlap of controls and privacy requirements

IC

- Customer data protection policies

ISO 27001

- A.18.1.4 – Privacy and protection of personally identifiable information

NRS

- 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....



SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

25

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. A.14.1: 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, public networks.	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



SCCETM

Society of Corporate Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

26

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



SCCE[™]

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

27

And here's some additional advice Overcoming roadblocks to your compliance initiatives



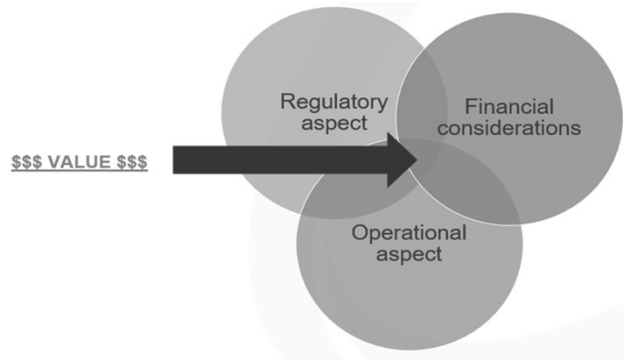
SCCE[™]

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

28

And one more

The sweet spot in your compliance recommendations



SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

29



Thank you very much



SCCETM

Society of Corporate
Compliance and Ethics 18th Annual Compliance and Ethics Institute 2019, National Harbor, Maryland

30