RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **IDP-F09V**

The Accountability Game: Streamlining Data Privacy Across APAC and the Globe

Robinson Roe

CIPP/E, CIPM
Managing Director, Asia Pacific
OneTrust

Jason Lau

CISSP, CIPP/E, CIPM, CGEIT, CRISC, CISM, CISA, CEH, CNDA, HCISPP
IAPP Fellow of Information Privacy (FIP)
Chief Information Security Officer
Crypto.com

Speakers

Jason is currently the Chief Information Security Officer (CISO) at Crypto.com where he drives the global cybersecurity and privacy strategy. Jason has over 20 years in consulting experience for Fortune 200 companies in Management Consulting, Cybersecurity, Data Privacy, Risk, Compliance and IT Governance. Travelled extensively and worked closely with organizations in Australia, Switzerland, Singapore, USA and HK.

CISSP, CIPP/E, CIPM, CGEIT, CRISC, CISA, CISM, CDPSE, CEH, CNDA, HCISPP, ITILv3, CSM, ISO27701:2019 Senior Lead Auditor and Senior Lead Implementer, ISO 27001:2013 Lead Auditor, Fellow of Information Privacy FIP by the IAPP

https://linkedin/com/in/jasonciso

Robinson Roe is the Managing Director of OneTrust for Asia Pacific, Japan. Prior to OneTrust, Rob was the Vice President and Managing Director of AirWatch by VMware for Australia & New Zealand. Previously Rob worked for Telstra(Australia), Gartner(USA), IBM(Asia Pacific, USA, Australia) and Vickers Ruwolt. Robinson holds a CIPP/E and CIPM from the IAPP.

rroe@onetrust.com
https://linkedin.com/in/robinsonroe

Agenda

I. Regulation in the New Growth Industry

II. Streamlining Data Privacy Case Study: ISO 27701

III. A Guide to ISO 27701 Certification

Regulations – the New Growth Industry

GDPR

CALIFORNIA CONSUMER PRIVACY ACT

Privacy Commissioner
Te Mana Mātāpono Matatapu

Japan Act of Protection of Personal Information

PDPA

CBPRs
CROSS BORDER PRIVACY RULES SYSTEM

China Cyber Security Regulations

OAIC

Australian Government
Office of the Australian Information Commissioner

ISO 27701

ISO 27001

NIST
National Institute of Standards and Technology

PCI DSS COMPLIANT

AICPA Service Organization Control Reports
AICPA SERVICE ORGANIZATIONS SOC
aicpa.org/soc
Formerly SAS 70 Reports

SIG SHARED ASSESSMENTS

CSA cloud security alliance®

ACCC AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Consumer Data Rights

Comprehensive Data Protection Laws

- **Australia** – Privacy Act & Privacy Principles
- **China** – Cybersecurity Law and the non-binding standard: Information Security Technology - Personal Information Security Specification (GB/T 35273-2017) (*Oct. 2020*)
- **Hong Kong** – Personal Data Privacy Ordinance
- **India** – Personal Data Protection Bill (*draft legislation*)
- **Indonesia** – Protection of Personal Data Bill (*draft legislation*)
- **Japan** – Act on the Protection of Personal Information
- **Macau** – Personal Data Protection Act
- **Malaysia** – Personal Data Protection Act
- **New Zealand** – Privacy Act & Information Privacy Principles
- **Pakistan** – Personal Data Protection Bill (*draft legislation*)
- **Philippines** – Data Privacy Act
- **Singapore** – Personal Data Protection Act
- **South Korea** – Personal Information Protection Act
- **Taiwan** – Personal Data Protection Act
- **Thailand** – Personal Data Protection Act

Agenda

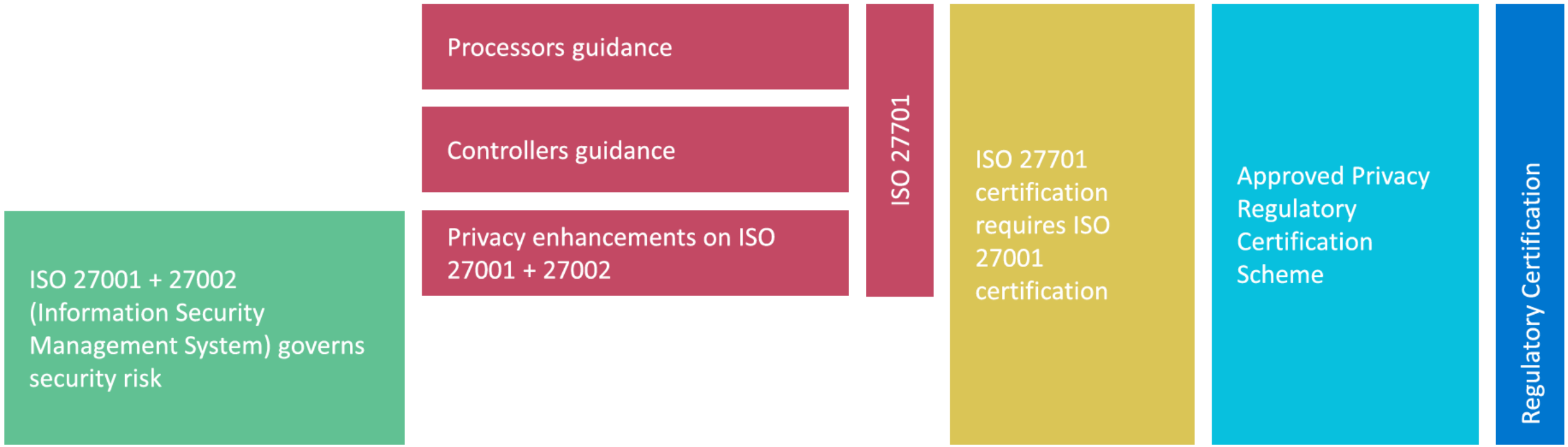
I. Regulation in the New Growth Industry

II. Streamlining Data Privacy Case Study: ISO 27701

III. A Guide to ISO 27701 Certification

Security vs. Privacy

Crypto's Journey to ISO 22701:2019



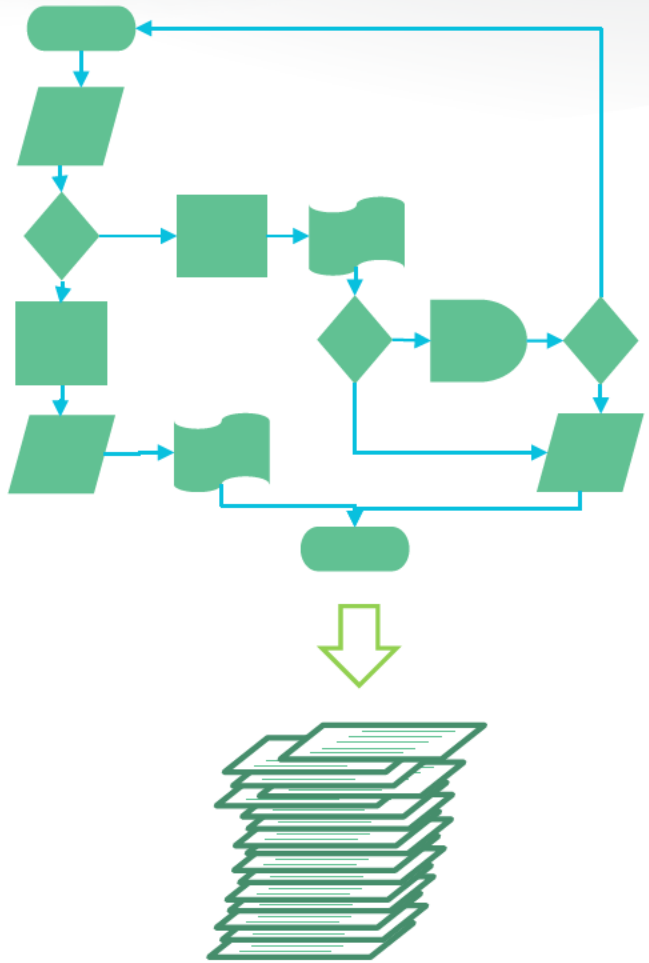
Agenda

I. Regulation in the New Growth Industry

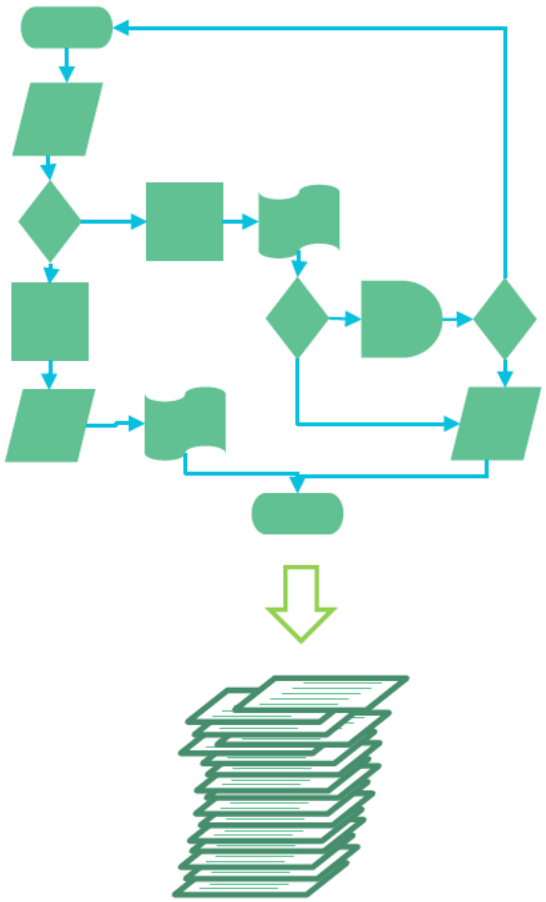
II. Streamlining Data Privacy Case Study: ISO 27701

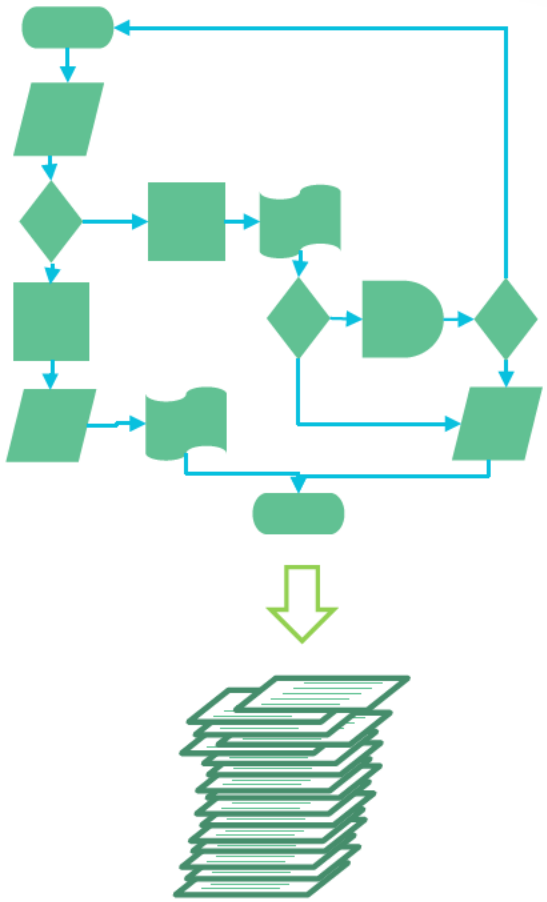
III. A Guide to ISO 27701 Certification

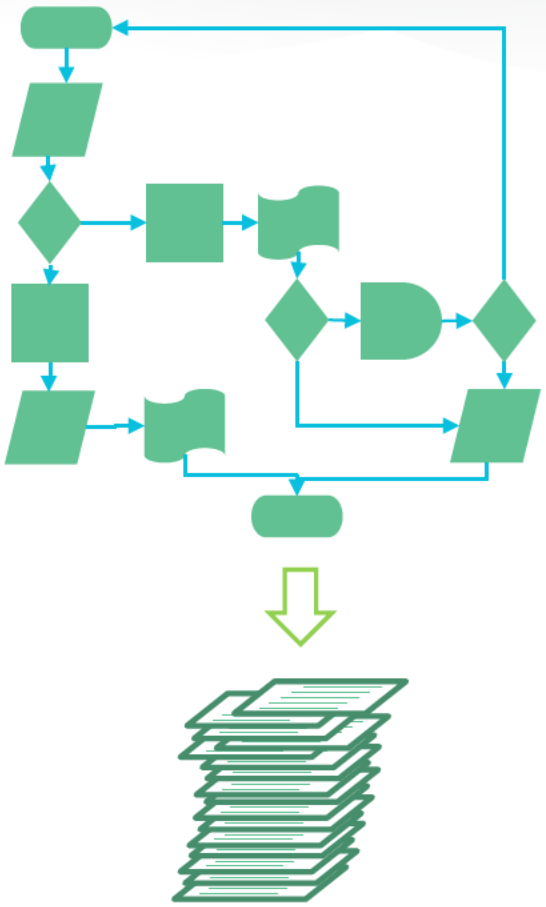
Semi-Manual Compliance Workflow

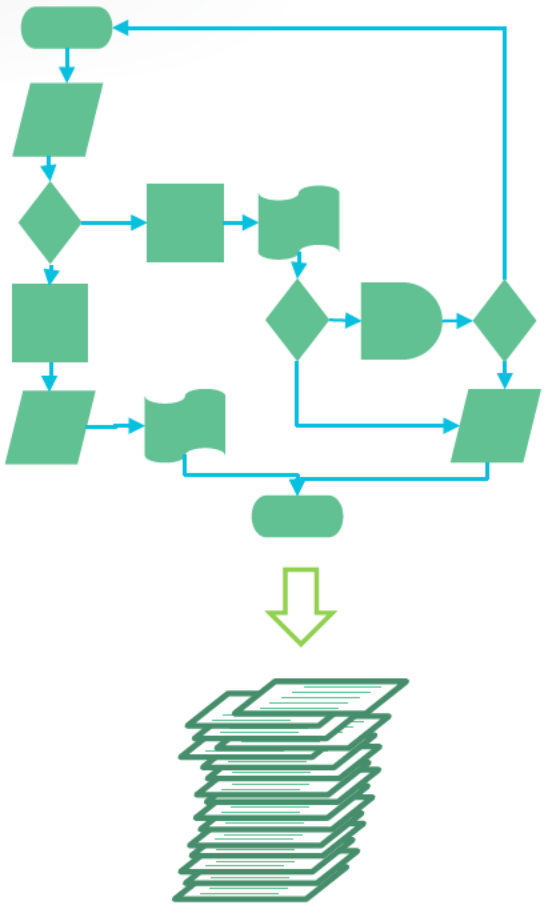


Regulation Semi-Manual Compliance Workflow: Privacy, Security, VRM, GRC



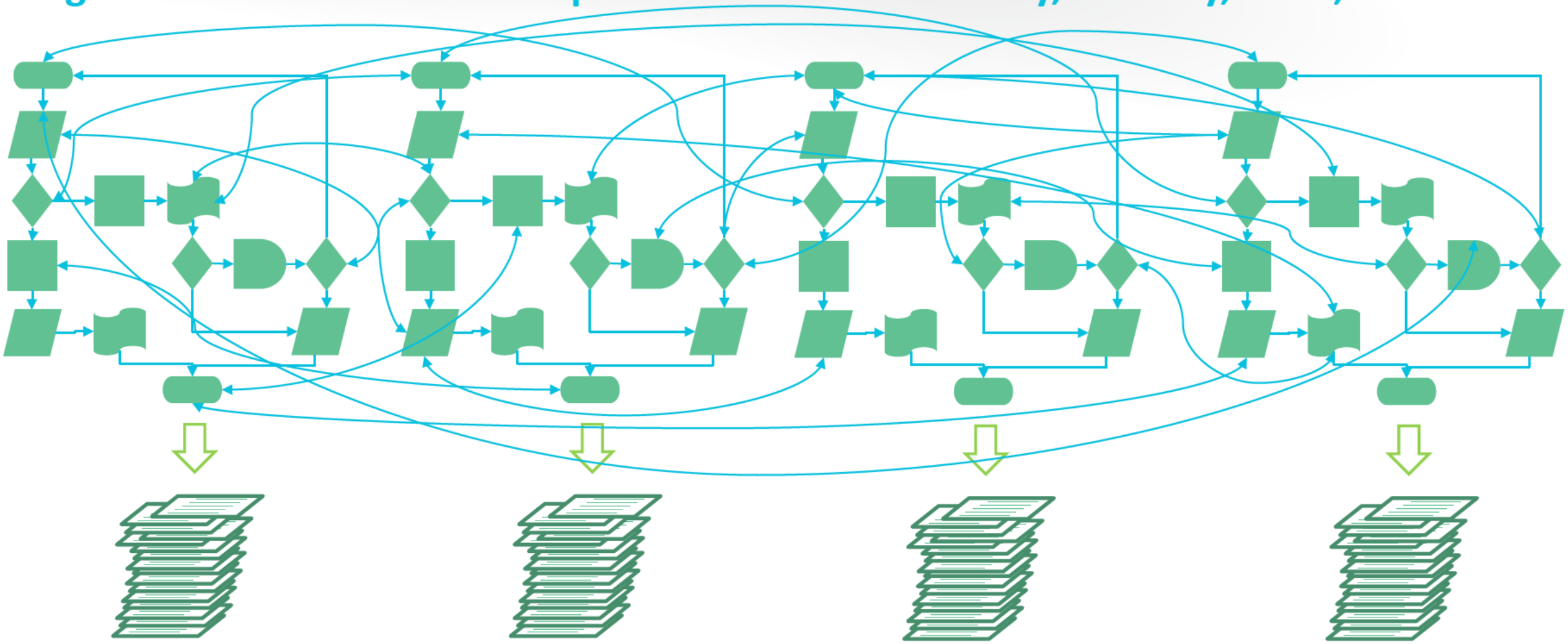






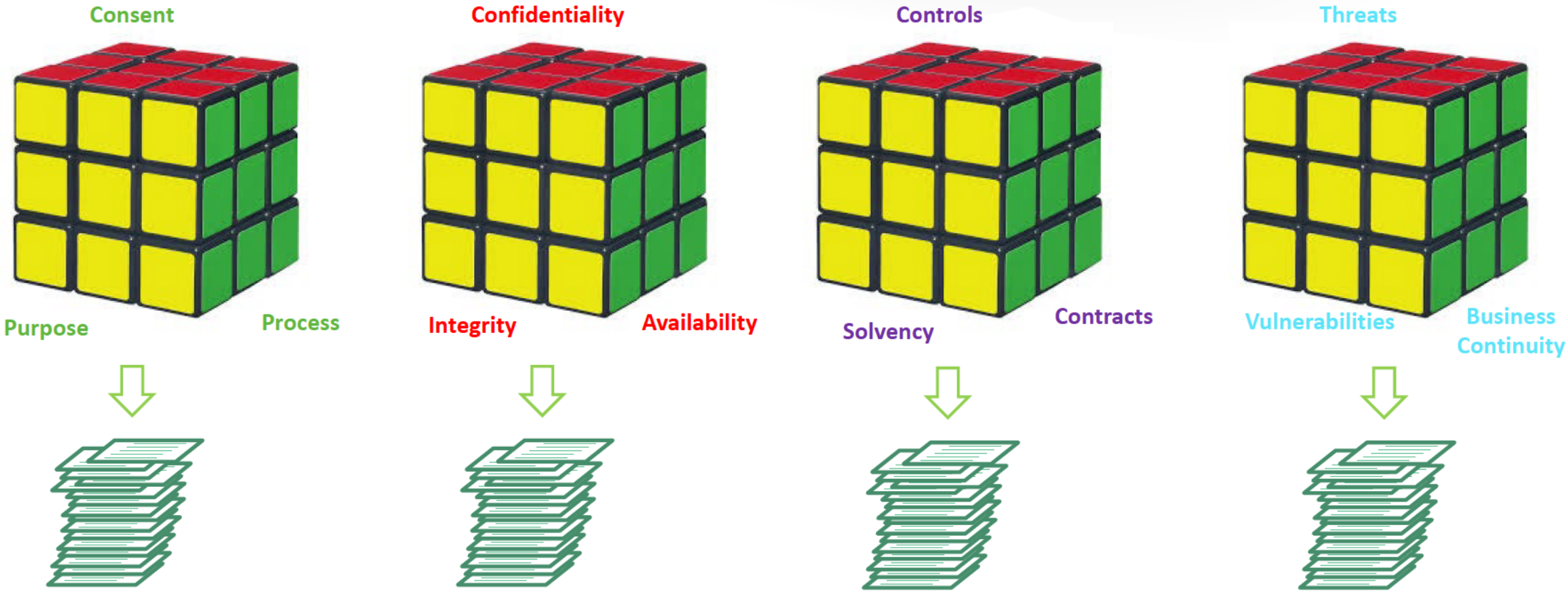
Privacy **Security** **Vendor Risk Management** **Risk & Compliance**

Regulation Semi-Manual Compliance Workflow: Privacy, Security, VRM, GRC



Privacy **Security** **Vendor Risk Management** **Risk & Compliance**

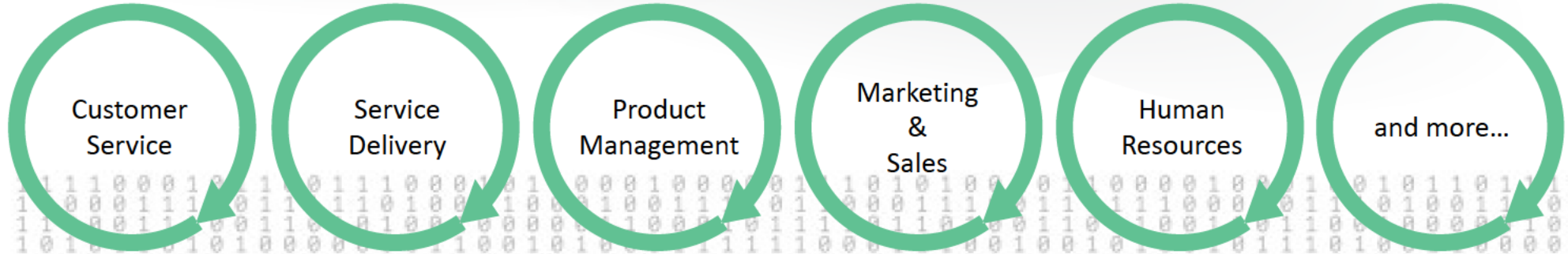
Regulation Semi-Manual Compliance Workflow: Privacy, Security, VRM, GRC



OneTrust PRIVACY, SECURITY & TRUST

crypto.com

Privacy, Security & Trust a Layered Perspective



Personal Data Organisational Data	What Data is being Collected?	For what Purpose?	Has Consent been given?	
Internal Systems / Assets	Where is the Data being Stored, Sent or Received?		Is it Safe?	Who has access?
3rd Party Systems / Assets	Are 3rd Parties Used?	Are their systems Secure?	Is there Contractual Coverage?	
Vendor Organisations	Are they Reputable/Solvent?	Where are they located?	Who are the Owners?	

Privacy, Security & Trust a Layered Perspective

Customer Service

Service Delivery

Product Management

Marketing & Sales

Human Resources

and more…

Personal Data

Organisational Data

Internal Systems / Assets

3rd Party Systems / Assets

Vendor Organisations

Consent

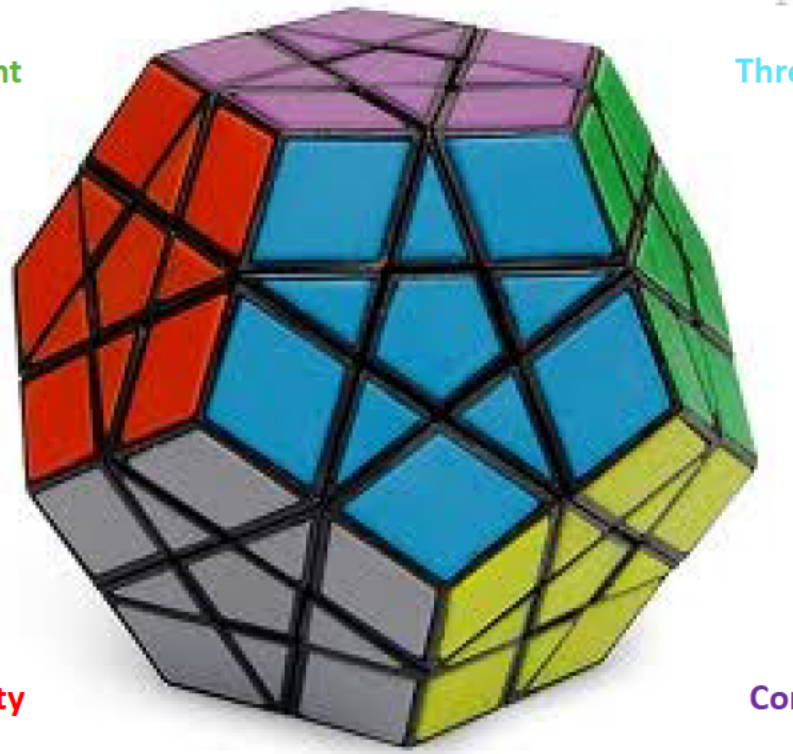
Purpose

Process

Confidentiality

Integrity

Availability



Threats

Vulnerabilities

Business Continuity

Solvency

Controls

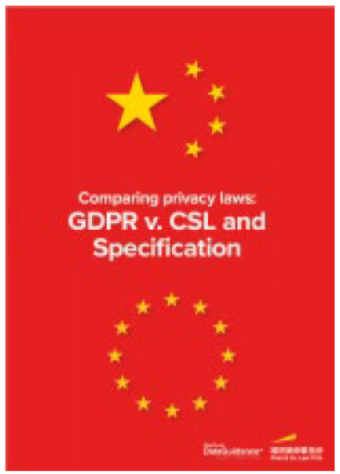
Contracts

OneTrust PRIVACY, SECURITY & TRUST

crypto.com

ISO27701 WhitePaper

DataGuidance: GDPR vs …



Apply What You Learned Today

- Learn about the privacy laws that impact your business
- Review ISO 27701 and see how it may help your privacy and security program
- Build an overarching privacy program that addresses global compliance requirements

RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

Questions?

Robinson Roe

CIPP/E, CIPM
Managing Director, Asia Pacific
OneTrust

Jason Lau

CISSP, CIPP/E, CIPM, CGEIT, CRISC, CISM, CISA,
CEH, CNDA, HCISPP
IAPP Fellow of Information Privacy (FIP)
Chief Information Security Officer
Crypto.com