OneTrust

Privacy Management Software

ISO 27001 & the GDPR: A Research-Based Approach to Identifying Overlap and Streamlining Efforts

Andrew Clearwater, CIPP/US, Director of Privacy, OneTrust

Introduction

Andrew Clearwater

CIPP/US

OneTrust

Director of Privacy

ISO 27001 & The General Data Protection Regulation

ISO 27001

33,000 organizations' information security management systems (ISMS) certified in 2016

Latest version published in 2013

Certification earned following successful audit

GDPR

In 2016, the GDPR was passed as law, effective May 25, 2018

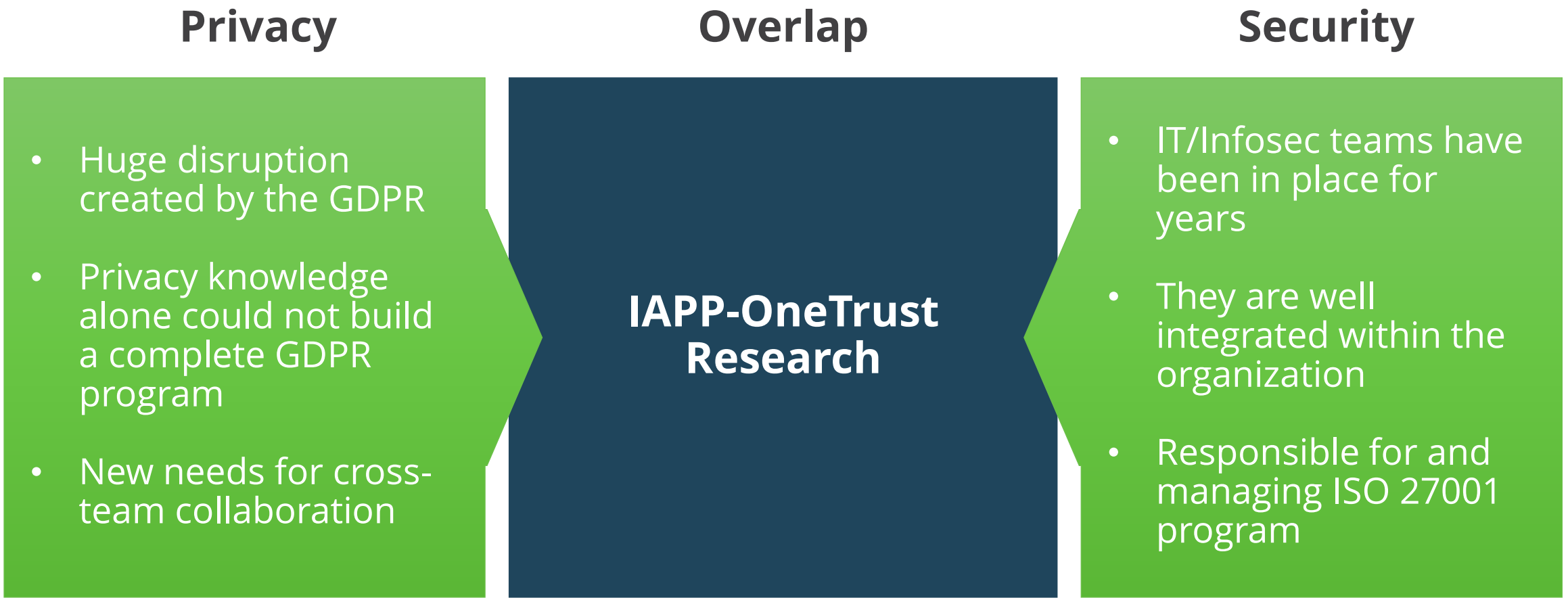
Biggest data protection overhaul of last 20 years

Replaces old data protection directive

Affects companies around the world

OneTrust
Privacy Management Software

Framing the Issue



Goal of the Research

1

Identify Overlap

How can existing work from security professionals be leveraged to support GDPR compliance?

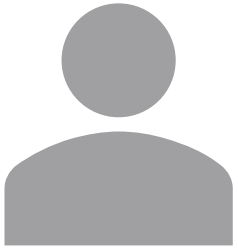
2

Map GDPR to ISO 27001

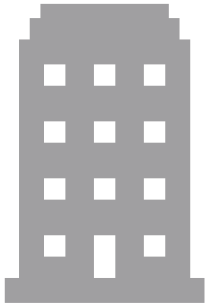
How does the ISO 27001 information security management framework correlate to the goals, objectives, and specific requirements of the GDPR?

Risk Management

Both aim at **reducing risk** to people and and organizations caused by **misuse of personal data**



GDPR:
Risk to Individuals



ISO 27001:
Risk to the Organization

Both call for organizations to invest in **knowledgeable leadership**

6 Critical Areas of Common Ground

1	Security
2	Breach Notification
3	Vendor Management
4	Recordkeeping
5	Data Protection by Design
6	Data Subject Rights

GDPR Terminology

1	**Personal Data**
2	**Processing**
3	**Controller**
4	**Processor**
5	**Personal Data Breach**
6	**Pseudonymization**

Security

The ISO 27001 Security Roadmap

Clause 4: organizations must determine both the internal and external issues that may affect their security programs

Clause 6: organizations must plan and structure a security program adequate to the scope identified. Create an information security risk assessment methodology.

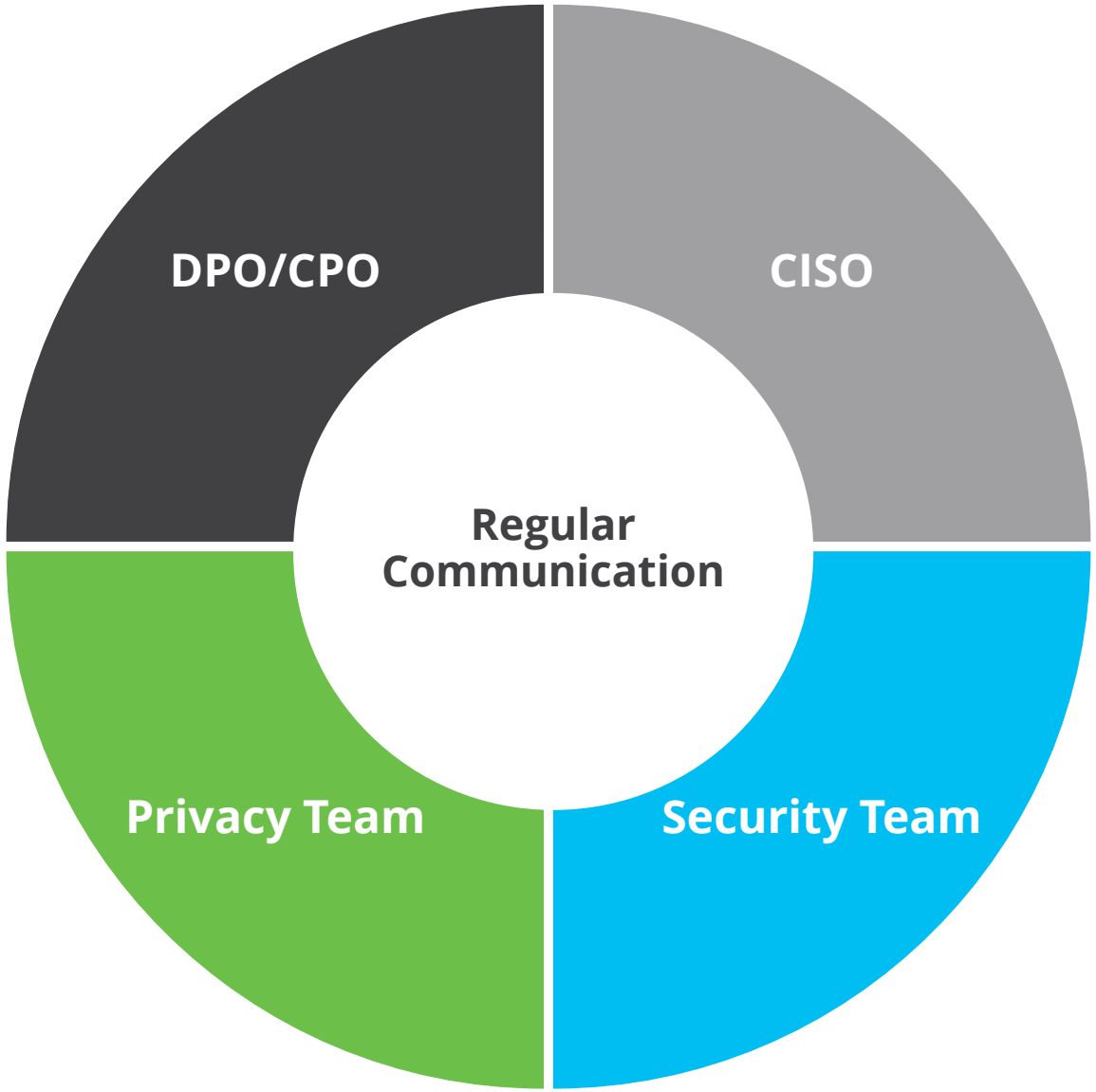
Clause 8: Implementation of the processes

GDPR: Appropriate safeguards and oversight

Article 5: Security is a fundamental privacy principle

Article 32: Implement technical and organizational measures to ensure a level of security appropriate to the risk

Collaboration



OneTrust
Privacy Management Software

Security - Internal Discussion Items

- What types of personal data are being collected, processed, and stored?
  - Is any sensitive personal data (racial or ethnic identifiers, biometric, healthcare, financial data, etc.) included in the above?
  - Is sensitive data treated with a higher level of protection?
- How are security controls and protocols documented? Are specific controls identified for specific categories of data or specific data processing activities?
- What methods are currently used to determine risk of loss of confidentiality, integrity, and availability? Do they include an assessment of the rights of the data subjects?
- Is personal data encrypted at rest and in transit? Does the organization have the capacity and practice to anonymize or pseudonymize personal data?
- Are privacy professionals invited to security team meetings, and vice versa?

Breach Notification

ISO 27001 Data Breach Response Plans

Mechanisms to identify security incidents

Mechanisms to report security incidents to the necessary established channels

GDPR Articles 33 & 34 Personal Data Breach Notifications

Notification requirements to Supervisory Authorities

Notification without undue delay, no later than 72 hours after becoming aware

Notification requirements to affected individuals

Breach Notification - Collaboration

1	Adapt the managerial reporting structure created by the ISO 27001 requirements to incorporate the relevant supervisory authority
2	Proper management channels for reporting an identified security incident to include the DPO
3	Collaboration to draft the notice, to include the necessary information

Breach Notification – Internal Discussion Items

As these policies are updated, IT professionals should consider the following questions:

- Is the organization functioning as a data controller or a data processor?
  - There may be multiple answers to this question. For example, an organization may function as a processor while handling customer information and a controller while handling HR information.
- Are data inventories managed in such a way that the appropriate reporting metrics can be easily identified in the event of a breach?
- Do plans and procedures include the involvement of the DPO (notably to identify whether an incident qualifies as a personal data breach within the definition of GDPR)?
- In the event of a breach, are any controls in place to mitigate the risk for affected data subjects?
- How can incident response plans accommodate the 72-hour notification period?

Vendor Management

ISO 27001 Vendor Control

Vendor oversight and control: Critical components of data security protocols

Clause 8

Clause 9

Other specific controls

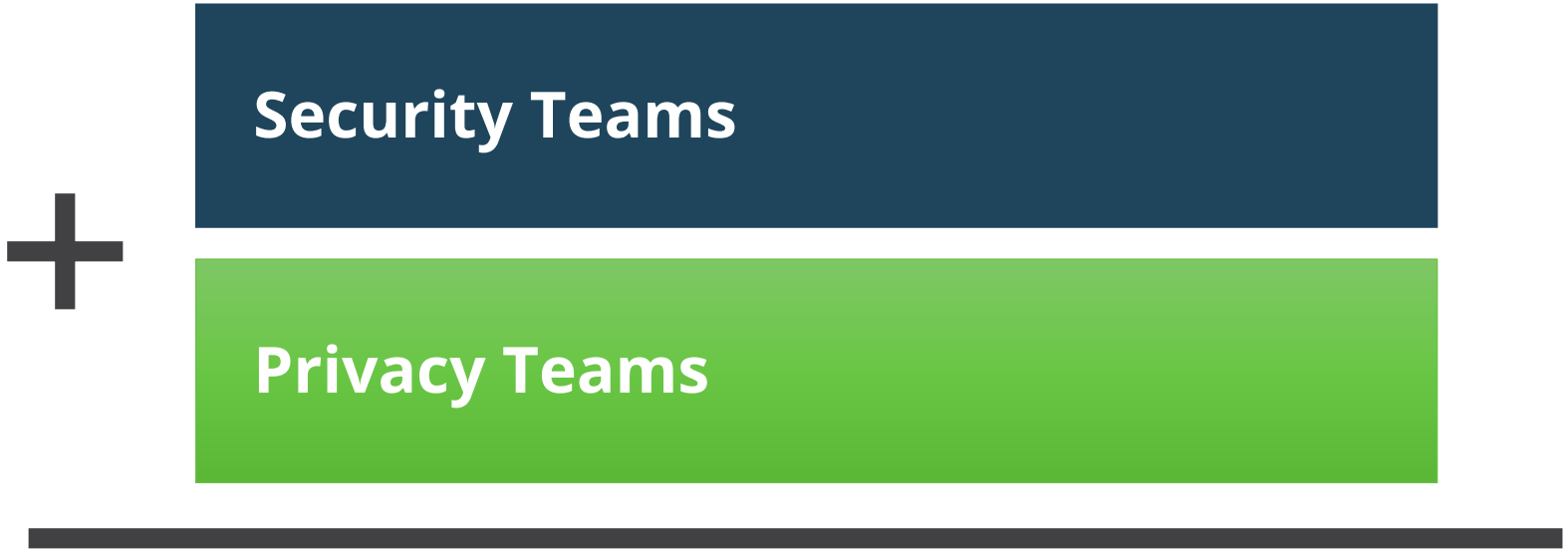
GDPR Article 28: Data Processors

New detailed requirements for vendor management

Use only vendors that can demonstrate appropriate security

Contractual requirements

Vendor Management - Collaboration



1. To determine if vendors provide appropriate levels of security

2. To incorporate security assurances in data processor contracts

OneTrust
Privacy Management Software

Vendor Management – Internal Discussion Items

- Does your organization have a comprehensive list of vendors and third party processors?
- Does your supplier risk assessment include data protection-related questions, including Article 28 requirements?
- Does your organization have standard data privacy contractual language?
  - If yes, is this language present in all third party contracts?
- When and if your organization is functioning as a controller, do you require processors to seek permission prior to using sub processors?
- When and if your organization is functioning as a data processor, are GDPR Article 32 security requirements part of your data security policies?

Recordkeeping

ISO 27001 Recordkeeping Requirements

Clause 8: Identify and label data assets (including ownership and acceptable uses for the data). Classifications, labeling and access controls of the data based on sensitivity level

Clause 9: Creation and maintenance of access control policy

GDPR Recordkeeping Requirements

Article 30: Controllers & processors are required to maintain records of their processing activities including items like:

Categories of data

Categories of data subjects

Safeguards

Cross-border data transfers

Recordkeeping - Collaboration

Recordkeeping – Internal Discussion Items

When reviewing security assets, it can help to document answers to the following basic questions:

- What type of personal data is collected?
- How and from where is the data collected?
- How and where is the data processed?
- How and where is the data being transferred?
- Is the data being stored, protected, and deleted?
- What data retention and destruction policies are already in place? Are they being followed?

Data Protection by Design

ISO 27001: A Flexible Security Framework

Clause 5: Development and periodic review of necessary security policies

Clause 6: Organizations must undertake ongoing security risk assessments

GDPR Article 25: Data Protection by Design and by Default

Incorporating security and privacy principles into products and processes from the outset and throughout implementation

Holistic view of data management

Data Protection by Design - Collaboration

Key component of data protection by design is produce and system design

The GDPR requirement of data minimization can be incorporated into existing security policies

OneTrust
Privacy Management Software

Data Protection by Design – Internal Discussion Items

- What personal data is required for each processing procedure handled by the organization or its processors?
- Do current policies and procedures limit the amount of personal data that can be collected through form limitations or other structural safeguards?
- Are developers or project managers on the security team? If so, how can they work more collaboratively with the privacy team to incorporate privacy principles into new products and services?

Data Subject Rights

ISO 27001 Data Categorization and Access Control Requirements

Clause 8: Data inventory, classification, and operating requirements

GDPR Data Subject Rights

Articles 13-22

9 Data Subject Rights

Detailed requirements about how to handle and respond to DSR

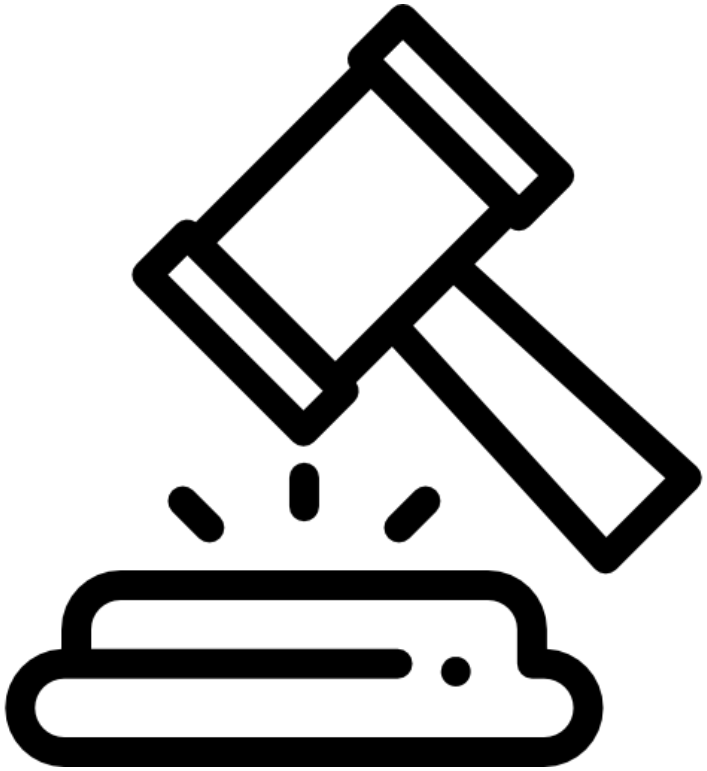
Data Subject Rights - Collaboration

Leverage existing data infrastructure to respond to data subjects' requests

Need transparency to understand company data processing practices

Need collaboration to understand categories of data collected and stored, its location and retention policies

Need involvement of security team (asset owners) to implement data subject request workflow



OneTrust
Privacy Management Software

Data Subject Rights – Internal Discussion Items

- What tags or markers do current data inventories and categorization schemes include?
  - What additional tags would be required to comply with a GDPR data subject request?
- Do current policies and procedures allow for data subjects to securely access any personal data your organization is holding about them? Are there other types of personal data that data subjects cannot automatically access? How will those reports be generated and communicated securely?
- Are there policies in place to review and correct outdated or otherwise incorrect information?
- Is there a policy or procedure in place to ensure that data subjects are notified when their personal data is changed or deleted?
- Does your organization use automated decision-making processes based on personal data?
- What data retention policies are in place and how are they enforced?
- Does the security team have an updated list of all external parties to whom personal data is transferred?

Get Access to the Research Today

Visit

onetrust.com/resources

to download the full research report today!

OneTrust

Privacy Management Software

Questions?