COPENHAGEN COMPLIANCE
Global GRC Solutions

GDPR Anniversary

Enhancing and Structuring the Sustainable GDPR Journey

Fred Oberholzer
EMEA Privacy Director and Group DPO
Canon

The Week in Ransomware - May 21st 2021 - Healthcare under attack

This week's ransomware news has been dominated by the attack on Ireland's Health Service Executive (HSE) that has severely disrupted Ireland's healthcare system.

LAWRENCE ABRAMS MAY 21, 2021

Air India data breach impacts 4.5 million customers

Air India disclosed a data breach after personal information belonging to roughly 4.5 million of its customers was leaked two months following the hack of Passenger Service System provider SITA in February 2021.

SERGIU GATLAN MAY 21, 2021

BLEEPINGCOMPUTER

COPENHAGEN COMPLIANCE
Global GRC Solutions

Fred Oberholzer

CIPP/E CIPM CIPT FIP CISA CISM

Canon EMEA Privacy Director and Group DPO

COPENHAGEN COMPLIANCE
Global GRC Solutions

Part 1: Why has the GDPR been successful?

Part 2: Where do I start?

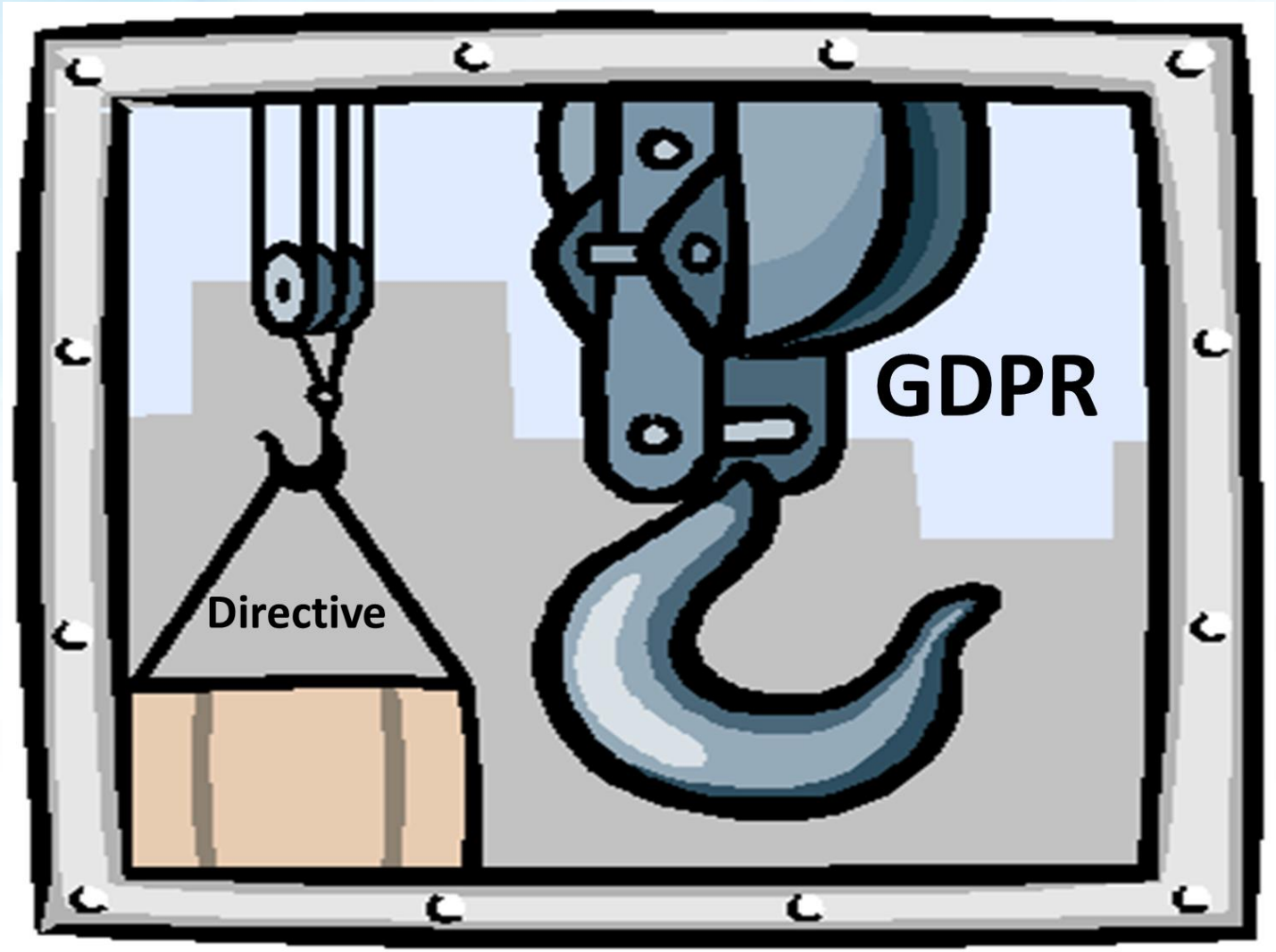
Part 3: How do I use these frameworks?

Part 4: What about ethics and culture?

COPENHAGEN COMPLIANCE
Global GRC Solutions

Part 1

Why has the GDPR been so successful?

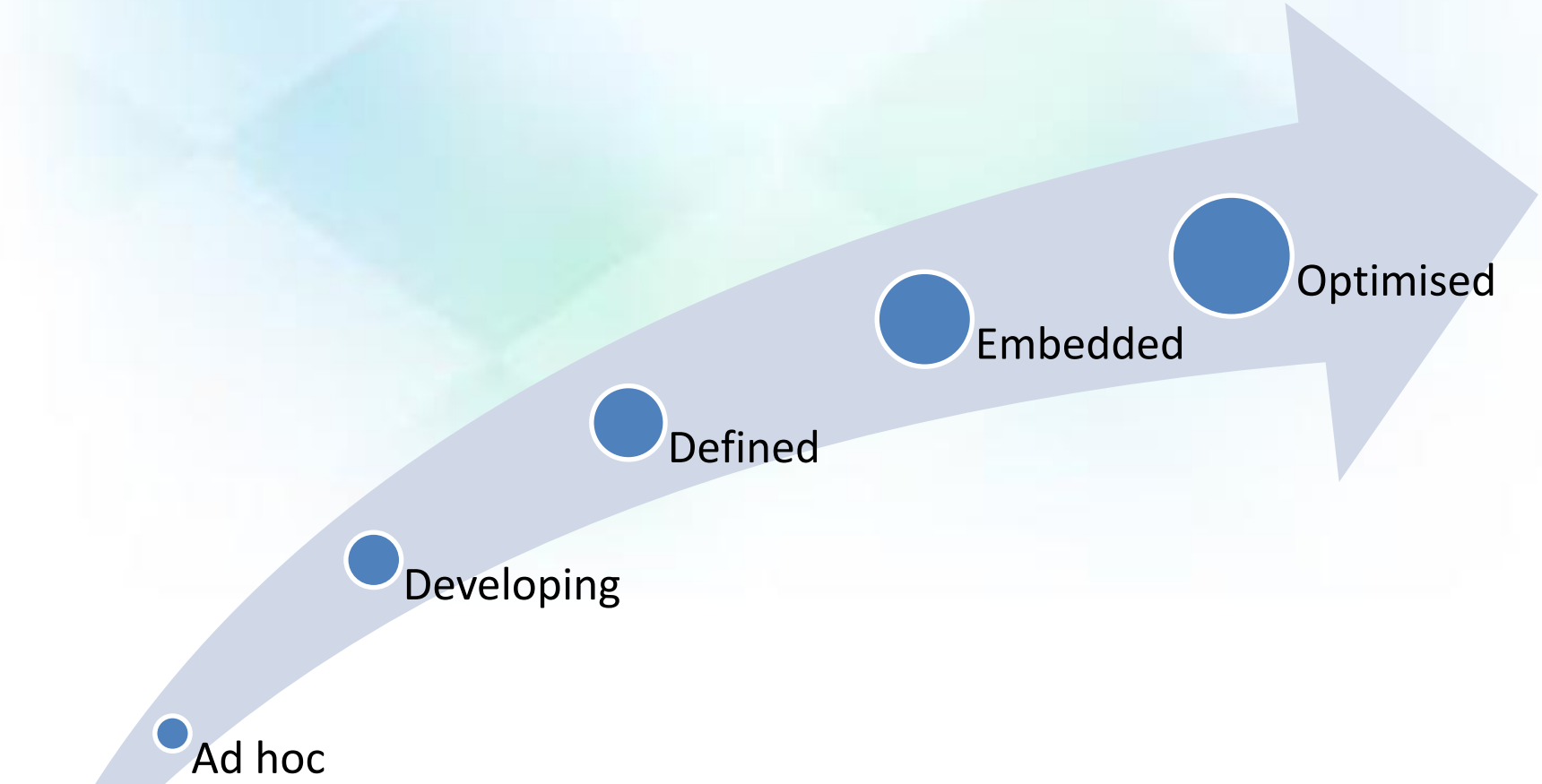


COPENHAGEN COMPLIANCE
Global GRC Solutions

Part 2

Where do I start?

Where are you on your compliance journey?



COPENHAGEN COMPLIANCE
Global GRC Solutions

If you don’t know where you are going, every road will not get you there

GDPR	GAAP
Lawfulness, fairness and transparency	**Notice** **Choice and Consent**
Purpose limitation	Collection
Data minimisation	Use, Retention and Disposal
Accuracy	Quality
Storage limitation	Use, Retention and Disposal
Integrity and confidentiality	Security for Privacy
Accountability	Management

GDPR	India PDP Bill
Lawfulness, fairness and transparency	(i) processing of personal data has to be fair and reasonable (iv) it should be lawful (v) adequate notice of the processing should be provided to the individual;; and
Purpose limitation	(ii) it should be for a specific purpose
Data minimisation	(iii) only personal data necessary for the purpose should be collected
Accuracy	(vi) personal data processed should be complete, accurate and not mis-leading
Storage limitation	(vii) personal data can be stored only as long as reasonably necessary to satisfy the purpose for which it is processed.
Integrity and confidentiality	reasonable security practices and procedures need to be maintained by each body corporate
Accountability	

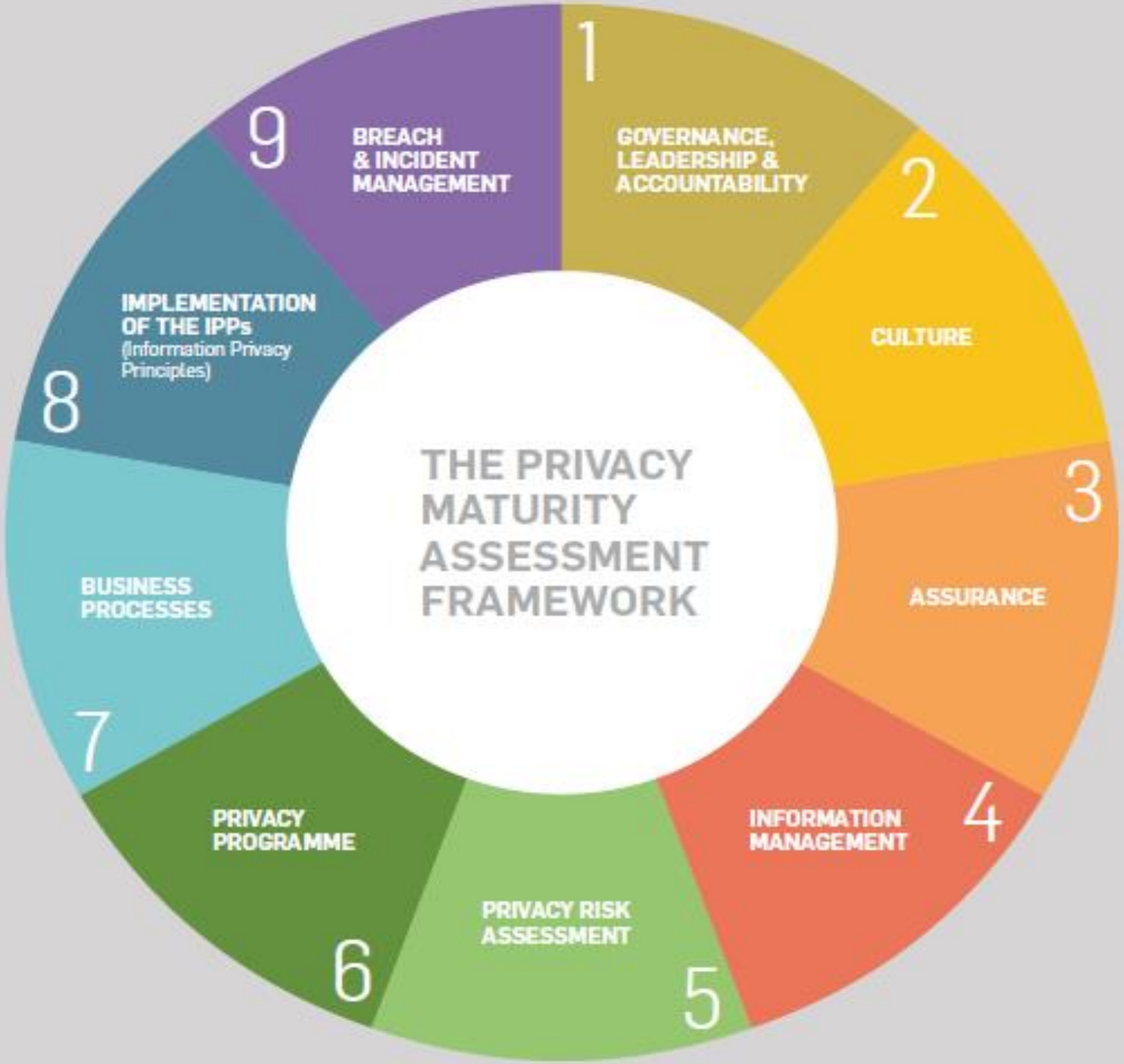
GDPR ≠ Privacy Management System

COPENHAGEN COMPLIANCE
Global GRC Solutions

- ISO/IEC 27701
- BS10012
- SOC2
- CIPL Accountability Framework
- TrustArc-Nymity Privacy and Data Governance Accountability Framework
- Standard Data Protection Model
- NIST Privacy Framework / SP800-53

Part 3

How do I use these frameworks?


THE PRIVACY MATURITY ASSESSMENT FRAMEWORK
1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT


1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs
(Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT

AD HOC	DEVELOPING	DEFINED	EMBEDDED	OPTIMISED
Unstructured approach where privacy policies, processes and practices are not sufficiently defined or documented. Privacy management is mostly dependent on initiatives by individuals rather than processes.	Privacy management is viewed as a compliance exercise and the overall approach is largely reactive with some documented guidelines. There is limited central oversight of the privacy policies, processes and practices with siloed approaches within business units.	Privacy policies, processes and practices are defined and comprehensive to meet the operating needs of the agency and are consistently implemented throughout. The business has a holistic and pro-active approach with widespread awareness of privacy management.	Privacy management is embedded into the design and functionality of business processes and systems and is consistent across the agency. Well-defined governance and oversight structures exist.	Privacy management is viewed as a strategic initiative with a clear agency culture of continual improvement. The agency is viewed by stakeholders and the public as a leader in privacy management, introducing innovative initiatives to meet their needs.

Part 4

What about ethics and culture?

COPENHAGEN COMPLIANCE
Global GRC Solutions

Ethics

Doing the right thing

COPENHAGEN COMPLIANCE
Global GRC Solutions

Culture

Winning Hearts and Minds

Summary

Thank You

COPENHAGEN COMPLIANCE
Global GRC Solutions