COPENHAGEN COMPLIANCE
Global GRC Solutions

How well is your privacy compliance/GDPR programme (really) going?

- Using assessing and audit to track your compliance/GDPR programme and its maturity

Fred Oberholzer FIP
EMEA Privacy Director and Group DPO
Canon

Global Data Protection Day by Copenhagen Compliance

JANUARY 28, 2022
ONLINE CONFERENCE

Assessing GDPR Compliance

COPENHAGEN
COMPLIANCE
Global GRC Solutions

COPENHAGEN COMPLIANCE
Global GRC Solutions

Fred Oberholzer

CIPP/E CIPM CIPT FIP

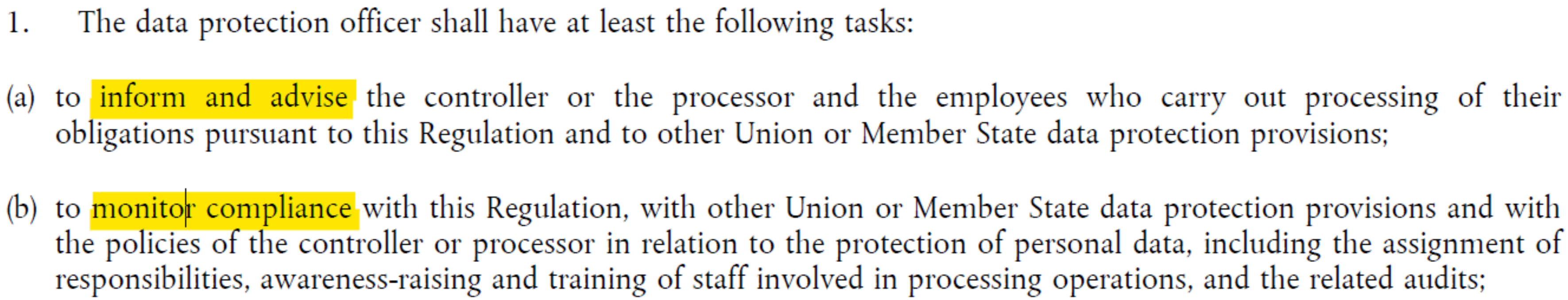
Canon EMEA Privacy Director and Group DPO

Member of IAPP Advisory Board

Why are assessments and audits important?

Where do you start?

If you don’t know where you are going, how will you know you have arrived?



1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

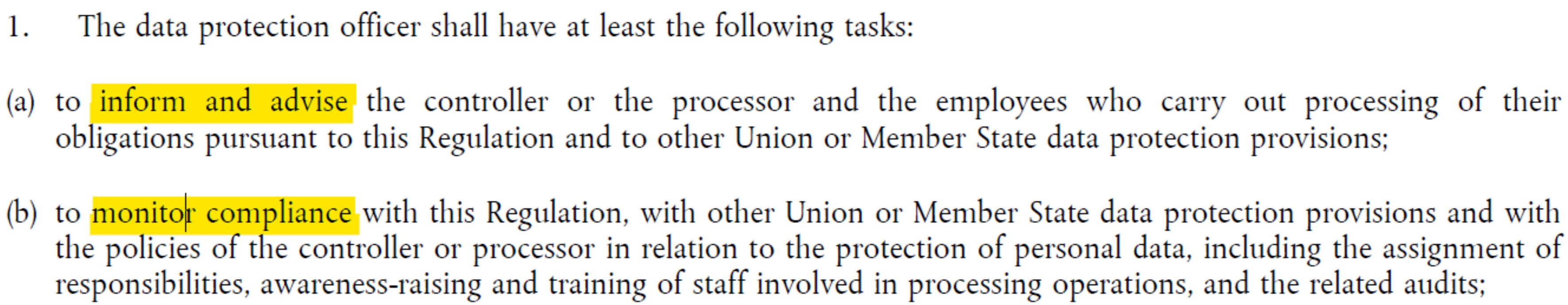
(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

Stakeholder Management

WHAT?

WHY?

Enforcement



1. The data protection officer shall have at least the following tasks:

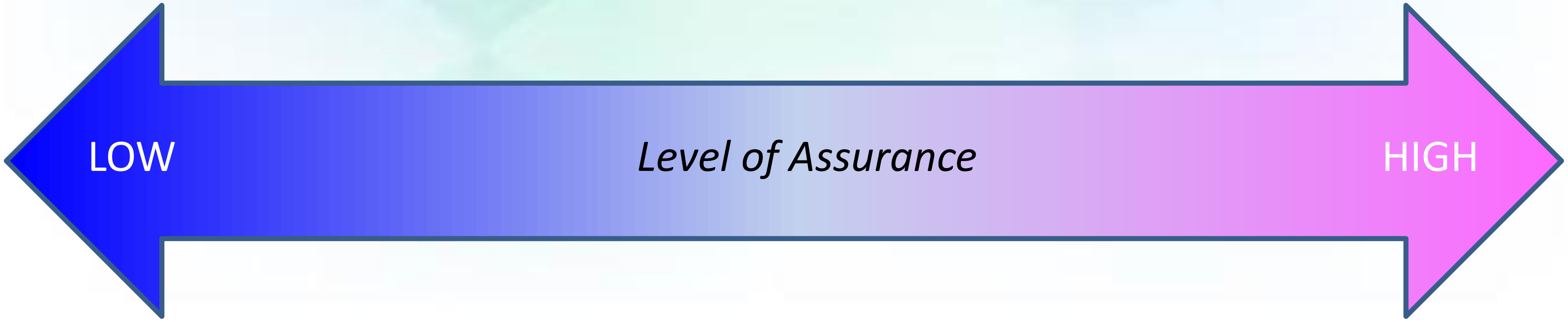
(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

Audit & Assessment Defined

Self-Assessment

Audit / Attestation

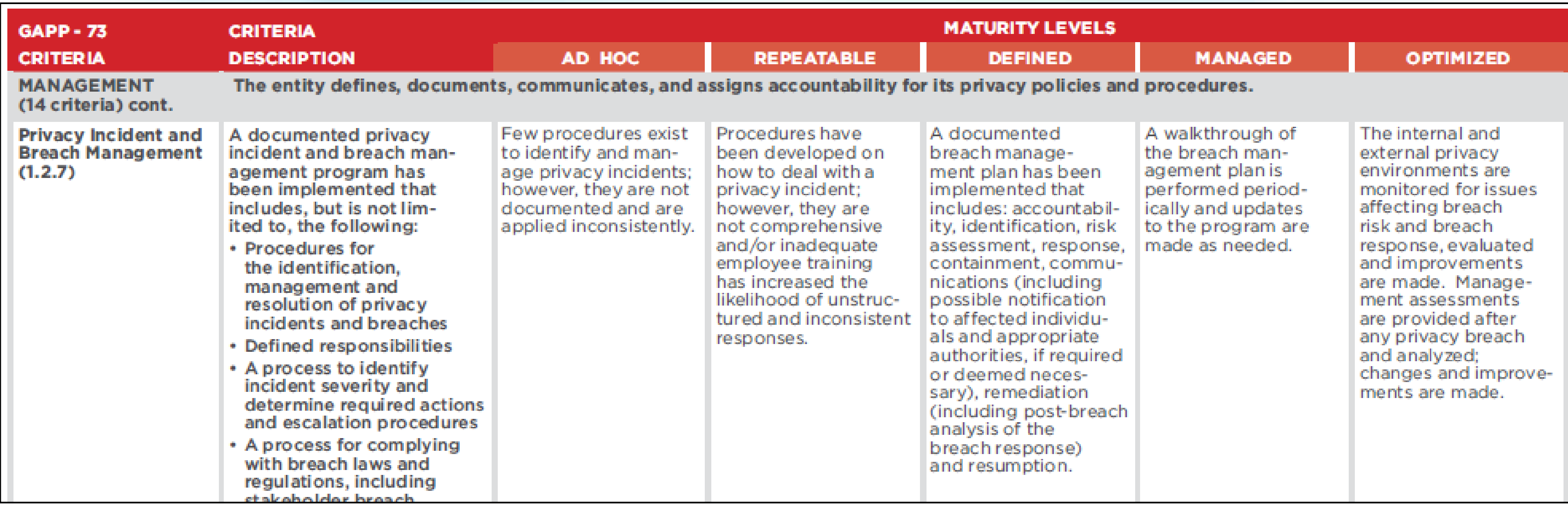


LOW

Level of Assurance

HIGH

GAAP Maturity Model



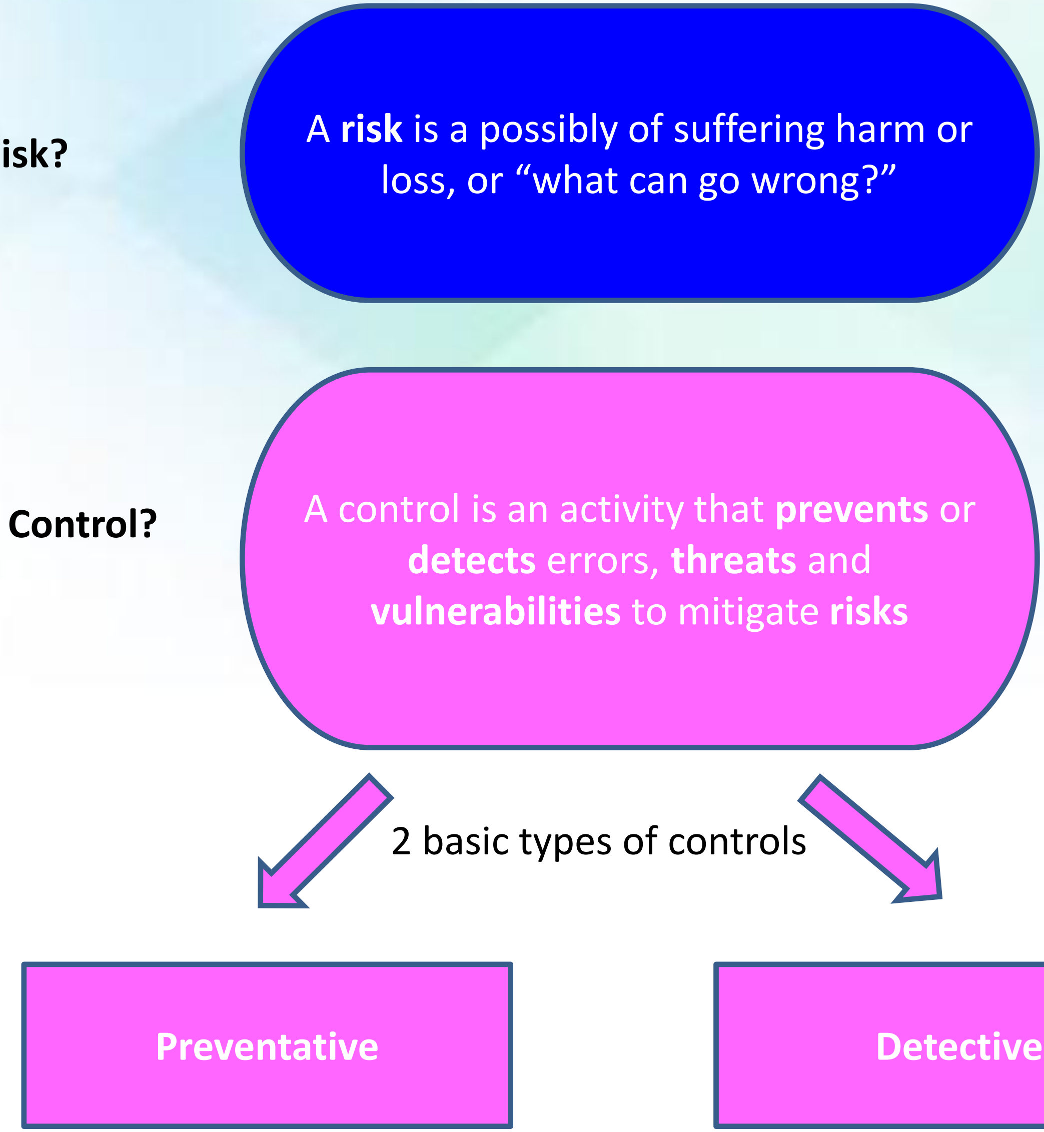
GAPP - 73	CRITERIA	MATURITY LEVELS				
CRITERIA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Privacy Incident and Breach Management (1.2.7)	A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following: • Procedures for the identification, management and resolution of privacy incidents and breaches • Defined responsibilities • A process to identify incident severity and determine required actions and escalation procedures • A process for complying with breach laws and regulations, including stakeholder breach	Few procedures exist to identify and manage privacy incidents; however, they are not documented and are applied inconsistently.	Procedures have been developed on how to deal with a privacy incident; however, they are not comprehensive and/or inadequate employee training has increased the likelihood of unstructured and inconsistent responses.	A documented breach management plan has been implemented that includes: accountability, identification, risk assessment, response, containment, communications (including possible notification to affected individuals and appropriate authorities, if required or deemed necessary), remediation (including post-breach analysis of the breach response) and resumption.	A walkthrough of the breach management plan is performed periodically and updates to the program are made as needed.	The internal and external privacy environments are monitored for issues affecting breach risk and breach response, evaluated and improvements are made. Management assessments are provided after any privacy breach and analyzed; changes and improvements are made.

COPENHAGEN COMPLIANCE
Global GRC Solutions

Risks and Controls

What is Risk?

What is a Control?



A **risk** is a possibly of suffering harm or loss, or “what can go wrong?”

A control is an activity that **prevents** or **detects** errors, **threats** and **vulnerabilities** to mitigate **risks**

2 basic types of controls

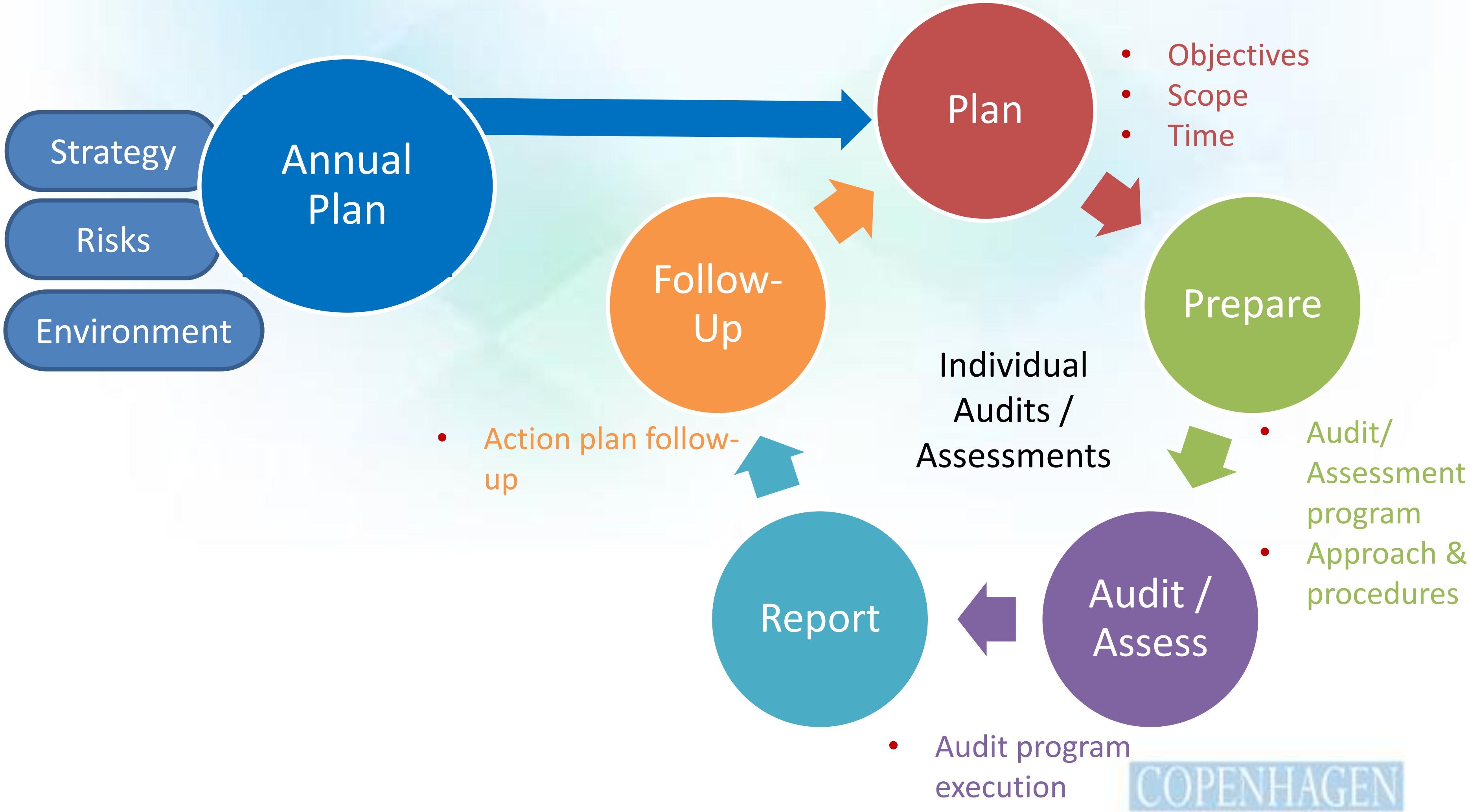
Preventative

Detective

Risk Treatment:
Risk Acceptance
Risk Avoidance
Risk Transfer
Risk Mitigation

COPENHAGEN COMPLIANCE
Global GRC Solutions

Assessment & Audit Lifecycle



- Objectives
- Scope
- Time

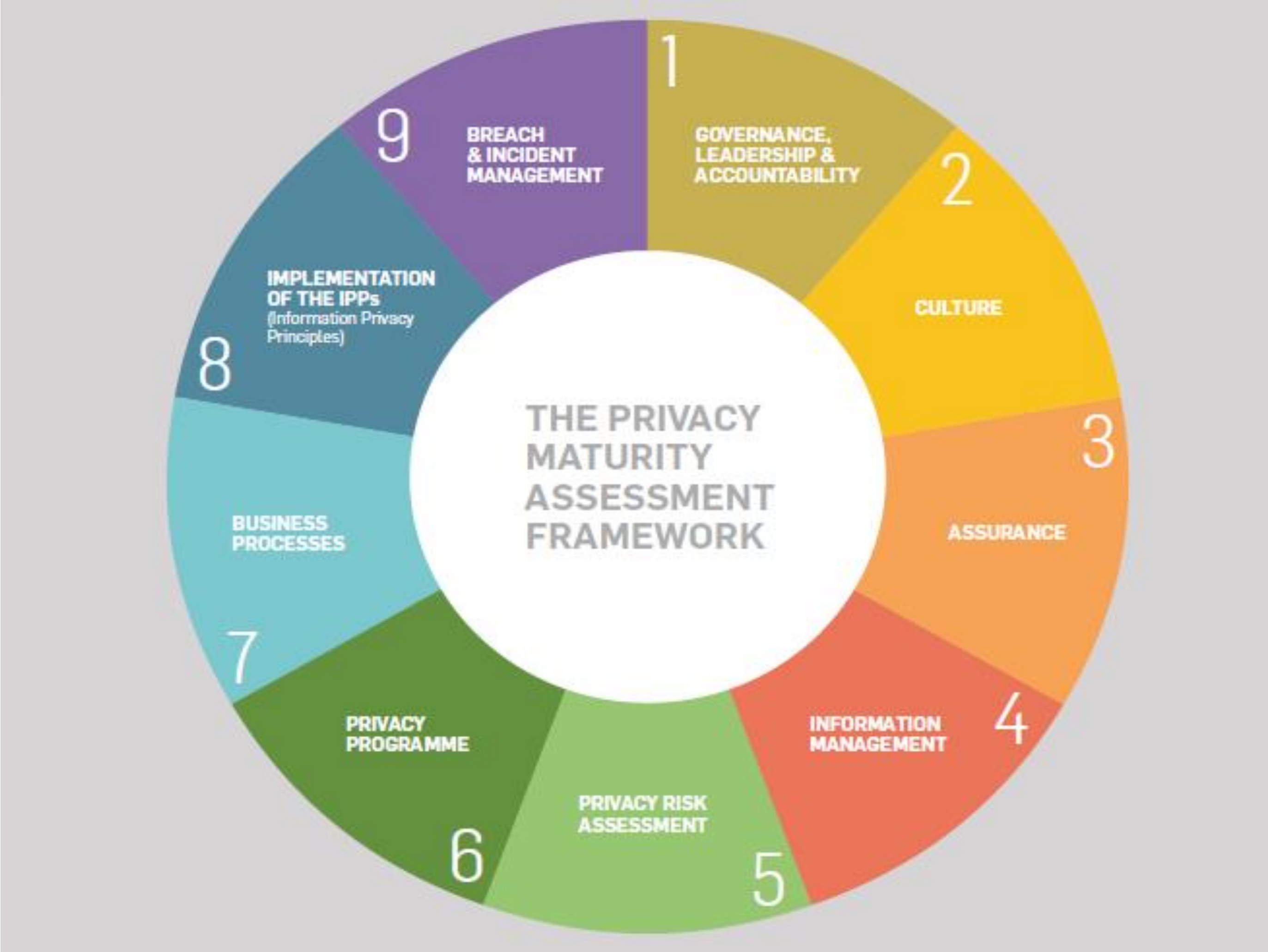
- Audit/ Assessment program
- Approach & procedures

- Audit program execution

- Action plan follow-up

COPENHAGEN COMPLIANCE
Global GRC Solutions

Maturity Assessments

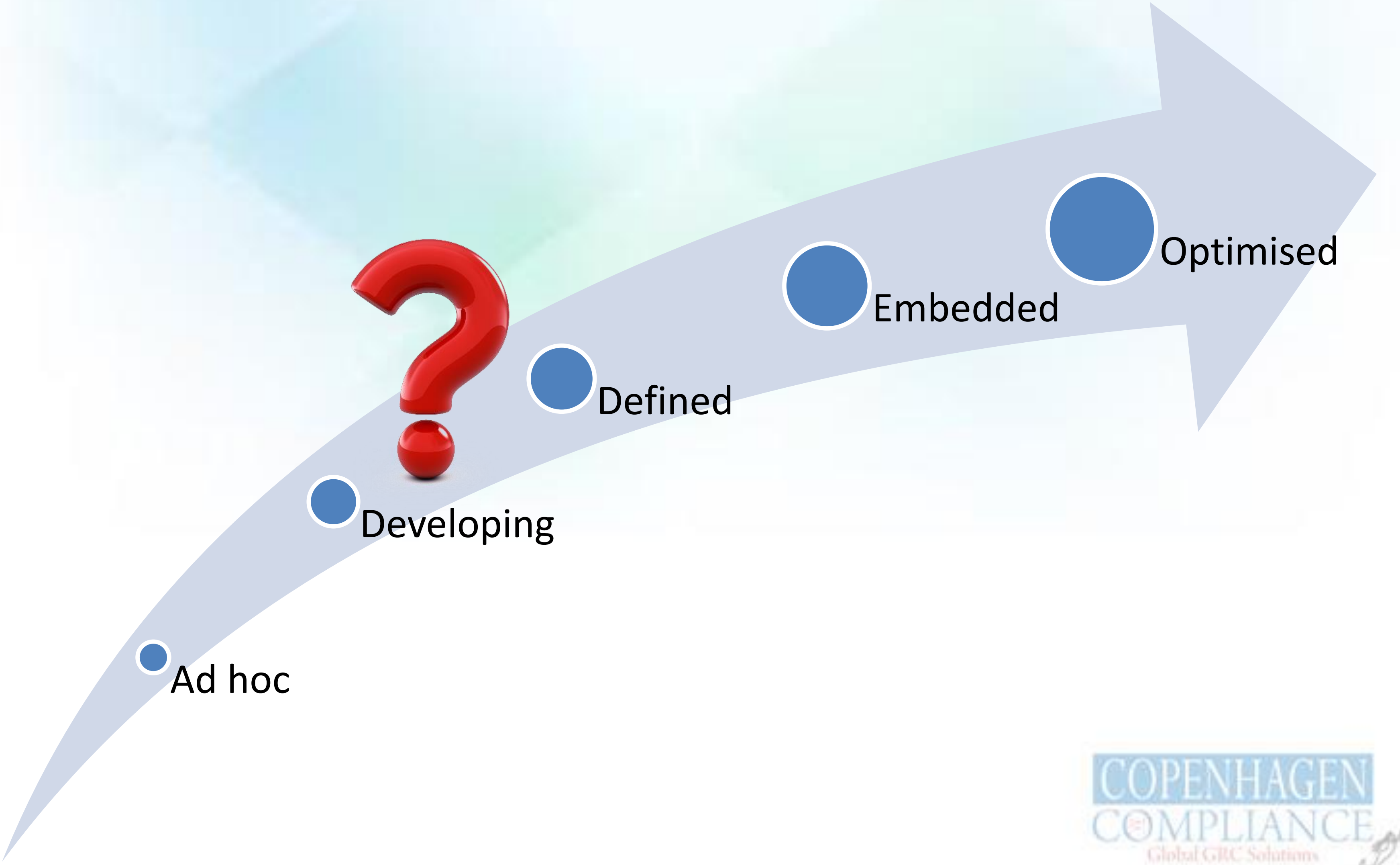

1
GOVERNANCE, LEADERSHIP & ACCOUNTABILITY
2
CULTURE
3
ASSURANCE
4
INFORMATION MANAGEMENT
5
PRIVACY RISK ASSESSMENT
6
PRIVACY PROGRAMME
7
BUSINESS PROCESSES
8
IMPLEMENTATION OF THE IPPs (Information Privacy Principles)
9
BREACH & INCIDENT MANAGEMENT
THE PRIVACY MATURITY ASSESSMENT FRAMEWORK

Principles

- Simple, pragmatic, easy to use
- Consistent assessment across organisation
- Scalable
- Risk management focused

COPENHAGEN COMPLIANCE
Global GRC Solutions

Where are you on your compliance journey?



Ad hoc

Developing

Defined

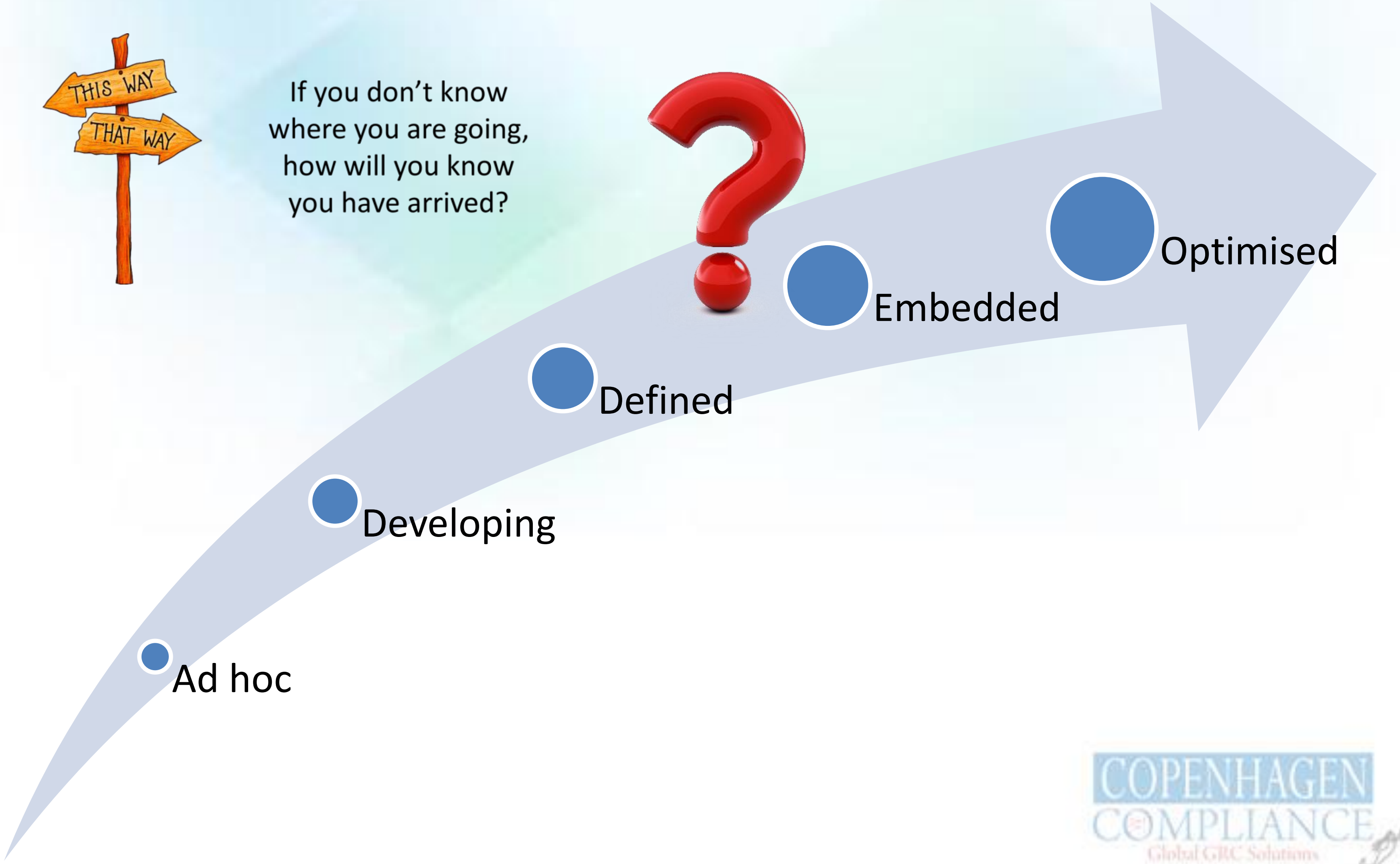
Embedded

Optimised

COPENHAGEN
COMPLIANCE
Global GRC Solutions

Where do you want to be?

If you don't know
where you are going,
how will you know
you have arrived?



Ad hoc

Developing

Defined

Embedded

Optimised

COPENHAGEN
COMPLIANCE
Global GRC Solutions

Privacy-by-Design

- Ann Cavoukian - "**7 Foundational Principles** of **Privacy-by-Design**"
- "reference framework - may be used for developing more detailed criteria for application and **audit/verification** purposes"
- **Principle 4 - Full Functionality – Positive-Sum , not Zero-Sum**

"Privacy is often positioned in a zero-sum manner as having to compete with other legitimate interests, design objectives, and technical capabilities, in a given domain. Privacy by Design **rejects** taking such an approach – **it embraces legitimate non-privacy objectives and accommodates them, in an innovative positive-sum manner**.

COPENHAGEN COMPLIANCE
Global GRC Solutions

Conclusion

Good Luck !