Service Organization Controls Reporting Event

Webinar| Session: 5

September 23, 2021

EY

Building a better working world

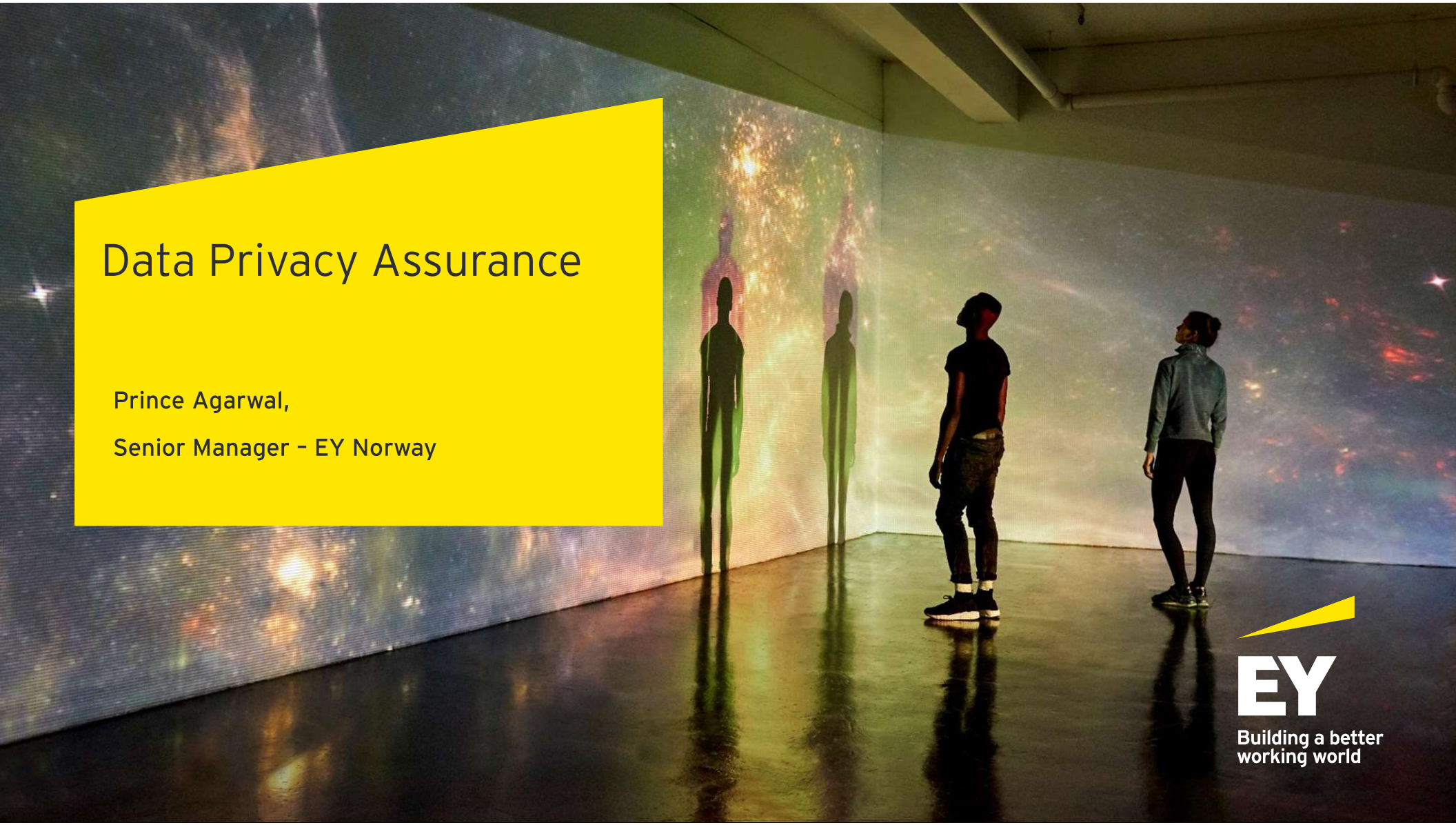
Agenda

1. Data Privacy Assurance
2. SOC Reporting as a Managed Service
3. Closing

Data Privacy Assurance

Prince Agarwal,

Senior Manager – EY Norway



Building a better working world

Agenda | SOC Reporting

1. Data protection history and Key drivers
2. Data protection across life cycle and privacy transformation
3. Assurance: Options
4. Brief Introduction to ISAE3000 GDPR

Data Protection History and Key Drivers

Data privacy and protection landscape evolution has been primarily regulation driven

Changing data privacy and protection regulatory landscape over time

1980s
- requirement for fair information practices as globalisation drove demand for regulations for transborder data flows
- over 50 million computers in use in the US

2000
- California implemented State Data Breach Notification Law.
- 1B PCs sold by 2002
- Social media (FB, YT) launched

2010
- The Federal Trade Commission (FTC) and National Credit Union Administration (NCUA) created the Red Flags Rule
- 1B smartphones bought by 2012

2015
- Adoption of digital technology and
- Online shopping becomes mainstream

2018
- The General Data Protection Regulation (GDPR) came into effect
- Digital transformation

Covid-19 Disruption

2020 onwards
- The California Consumer Privacy Act (CCPA) came into effect
- Use of IoT, AI/ML

Increasing pace of digital transformation

EY

Key Trends over time

1 More legislation to follow in coming time as developing countries will have their own privacy regulations.

2 More Focus from regulators with stricter scrutiny of businesses

3 More use of Privacy Tech Solutions

4 With use of AI/ML, IOT and Cloud, more focus on data protection and automated monitoring.

GDPR Enforcement

Since the three years post GDPR came into effect, consumers have become increasingly aware of their data privacy rights. As per Forrester reports, nearly half of companies still fall short of meeting GDPR and other data privacy requirements.

835

actions carried out by European data protection authorities.

275K+

complaints received by EU/EEA supervisory authorities (SAs) between 25 May 2018 and 30 November 2019.

Ignoring GDPR and upcoming data privacy regulations puts your brand at risk

4% Of your annual revenue

Penalties alone can run up to 4% of annual revenue with the cost of settling class-action lawsuits and losing customers due to legal action can be even higher.

68%

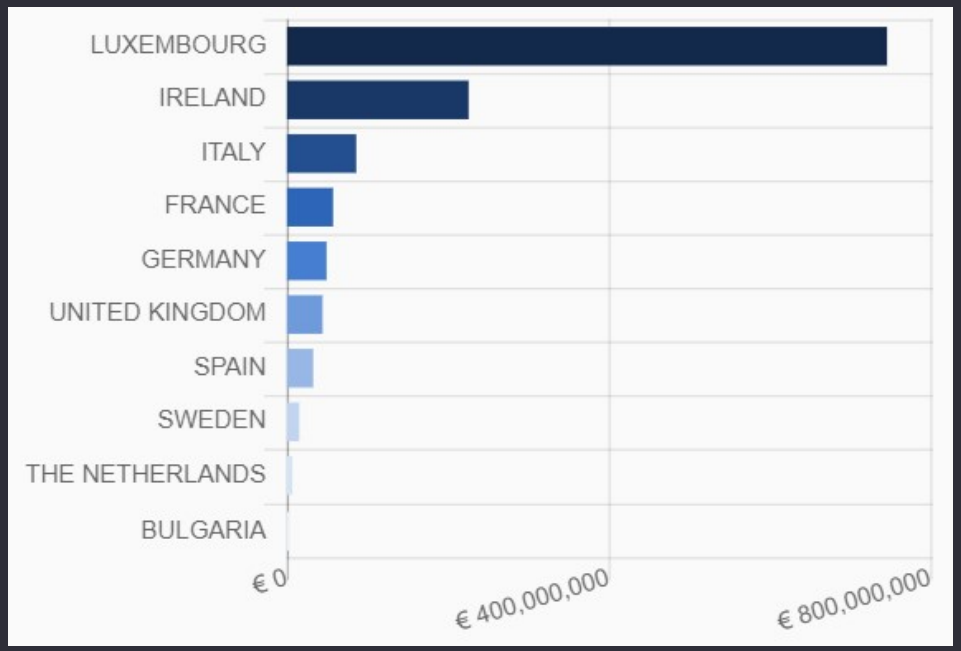
of US online adults are not comfortable with companies sharing and selling information on them and their online activities. The regulatory lawsuits can hit your brand and its reputation instantly.

Source: European Data Protection Board, Forrester, Enforcement Tracker

EY

GDPR Penalties in the EU

Top10 Countries and Total value of GDPR fines imposed from May 2018 to Sep 2021 (Euros)



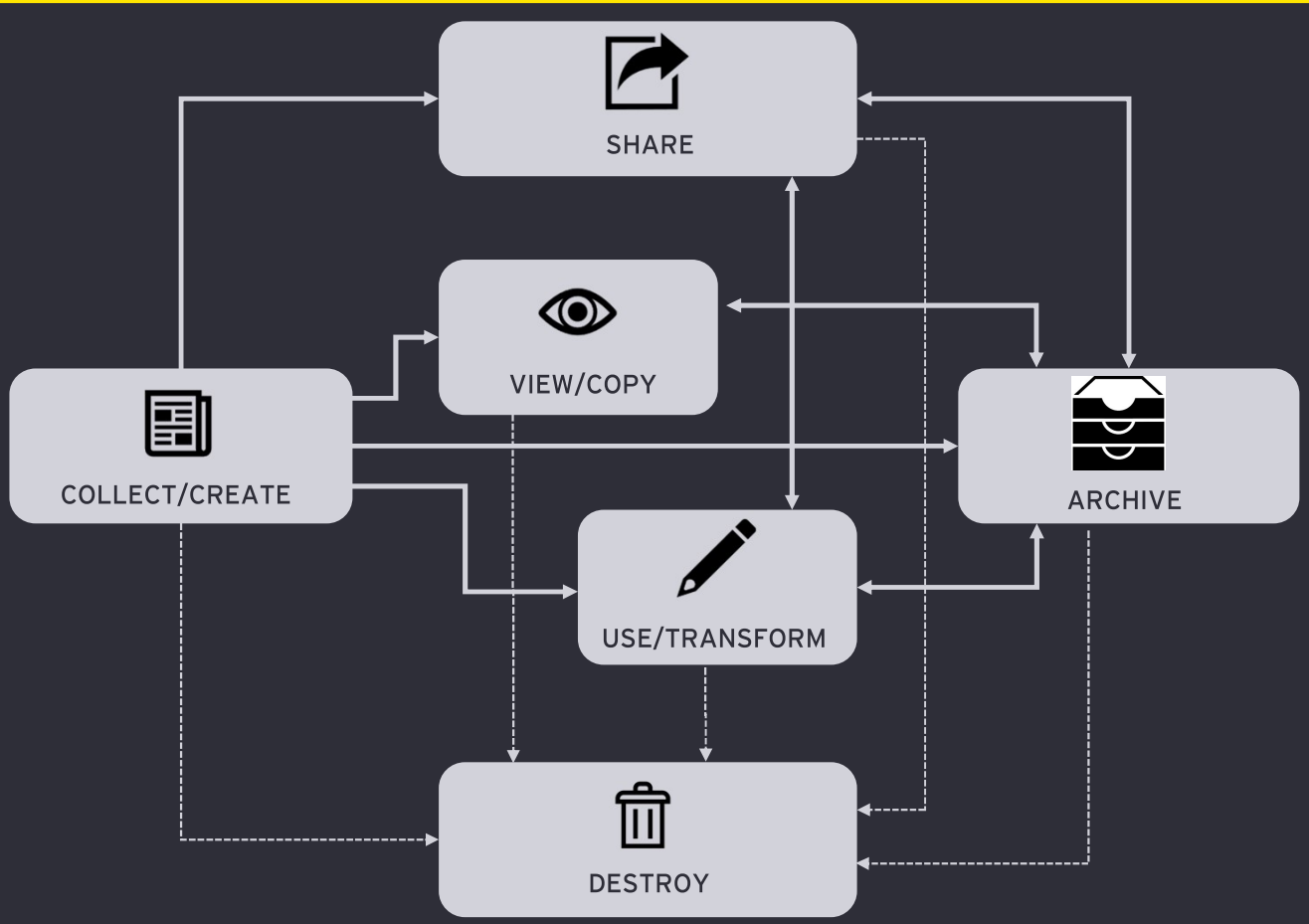
Source: GDPR Enforcement Tracker;

Top GDPR Fines in 2020-21

amazon

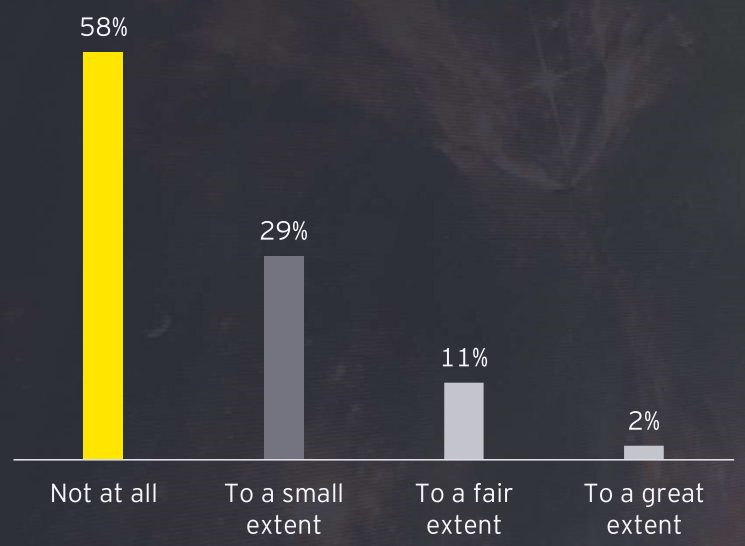
BRITISH AIRWAYS

Data Protection across life cycle



Privacy transformation in response to COVID-19 pandemic

Most organizations think that COVID-19 pandemic has not side lined privacy priorities



Has COVID-19 pandemic lowered the priority of privacy?

Key findings

45%

Organizations adopted new tech or contracted new vendor to enable remote work

30%

Organizations have been asked to share aggregated/anonymized COVID-19 pandemic data with a third party

19%

Organizations have shared the names of employees diagnosed with COVID-19 pandemic with other employees or the government

50%

Telecom, health and government entities have been asked to share anonymous data to combat COVID-19 pandemic.

Privacy in the wake of COVID-19 pandemic – Read the full report from here.

EY

Key considerations for privacy professionals

Are we providing staff with the right support and oversight?

Which systems and processes have changed?

Are my new reports based on the right data?

Are my staff aware of their responsibilities over personal data?

Do my staff have the right skills to reliably deploy new business solutions?

Do I have the right to collect and use the additional personal data?

Have we changed the internal control environment?

Do I need to update my privacy notice?

EY

Key findings: IAPP-EY Annual Privacy Governance Report 2019

41%

Compliance with privacy laws and regulations tops privacy professionals' priority list

58%

Of EU respondents mentioned GDPR Compliance to be topmost priority

38%

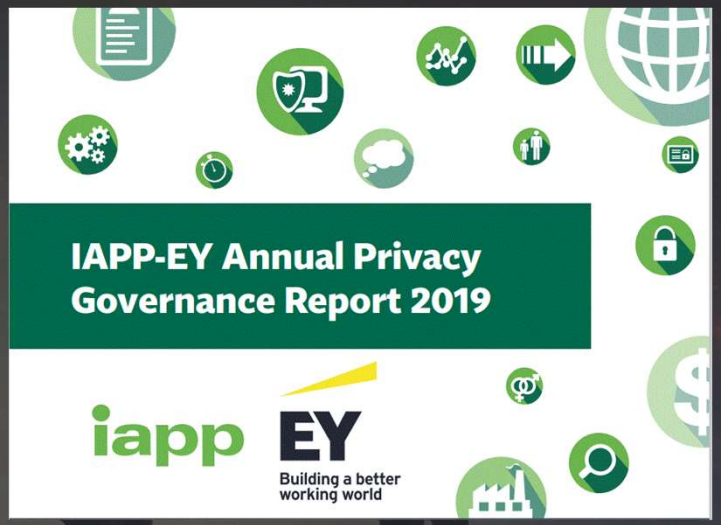
Organizations reported data breaches in 2019 compared to mere 18% in 2018

90%

Nearly all respondents (90%) report their firms rely on third parties for data processing, and the top method for ensuring vendors have appropriate data protection safeguards is "relying on assurances in the contract" (named by 94% of respondents).

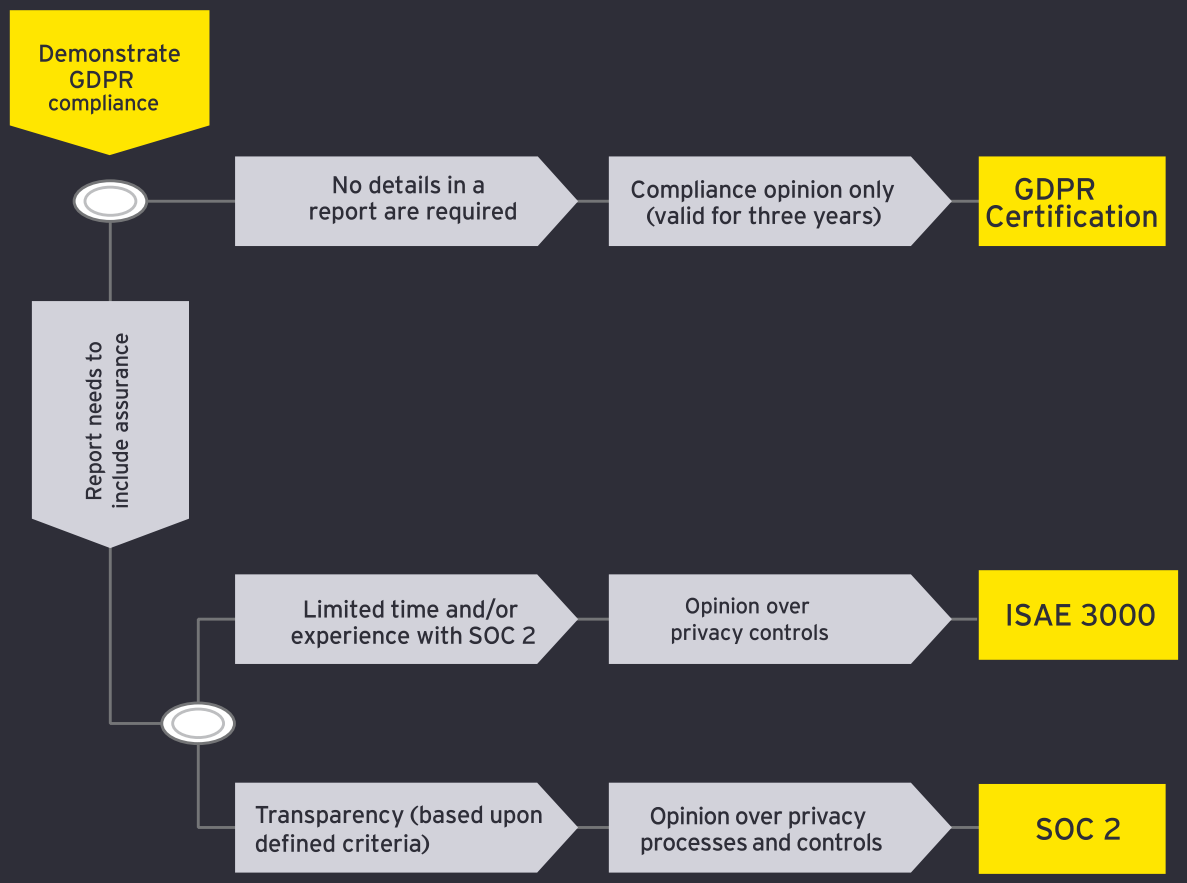
56%

respondents named "locating unstructured personal data" as the most difficult issue in responding to data subject access requests (including access, deletion, and rectification requests)



EY

What does your organization need?



How to build trust and assurance with stakeholders

Trust

Verify

- **ISO based certification**
  Confirms that there is a management system in place by focusing on policies and guidelines and does not require extensive testing of control effectiveness. These standards are code of practices and not GDPR specific.

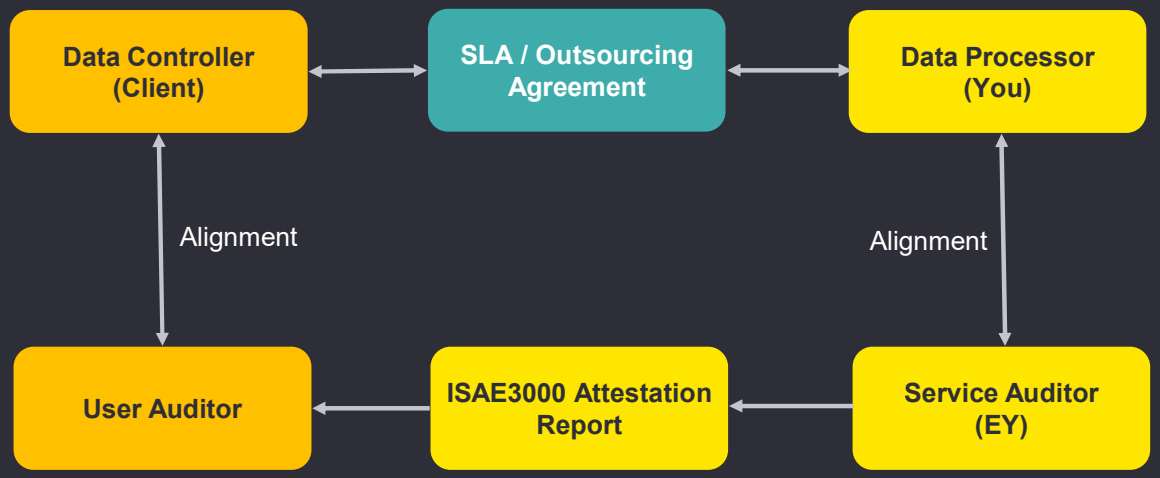
- **Data balance sheet**
  An extension to the privacy statement which creates transparency to use of personal data. It does not include an assertion on the effectiveness of data protection practices or controls.

- **GDPR certification**
  One-page statement stating the conformity to the requirements in the GDPR, which demonstrates that the business's privacy processes have been audited, but does not include detailed disclosure.

- **Third party reports (SOC2/ISAE3000)**
  Confirms also that the specified controls have been designed and are operating effectively.

EY

ISAE3000 attestation (Key Terms)



- Data Controller (Clients)
- Data Processor (you)
- User Auditor (Client's Auditor)
- Service Auditor (EY)

- The structure of the GDPR ISAE 3000 is following the standard requirement for ISAE reports which provides reliability and predictability.

Overview of Key Domains

Data Protection by Design and Default (Article 25)

Records of Processing Activities (Article 30)

Risk management (Article 35)

Breach Management (Article 33)

Cross Border Data Transfer (Article 44-47)

Representation of Processors (Article 27)

Code of Conduct (Article 40)

Data Subject Request (DSR)

Vendor Due-Diligence & Sub-processors

Storage and Retention

Article 28

Security Management

Onboarding Process

Change and Configuration Management

Event Monitoring, and Problem Management

IAM and PAM

Vulnerability Management

Log Management

Trainings, and Knowledge Management

Article 32

Data Protection – Appointment of DPO (Article 37 & 39)

EY

Approach for Attestation Report

Planning

Identify Scope, expectations and prepare high level plan with key stakeholders

Walkthrough

Review process descriptions, control descriptions and risks to assess control design

Testing

In depth examination and testing of controls with sample selection to assess operating effectiveness

Reporting

Quality Assurance, issue of formal report, customer communication and lessons learnt

Lessons Learnt

Recommendations and Improvements

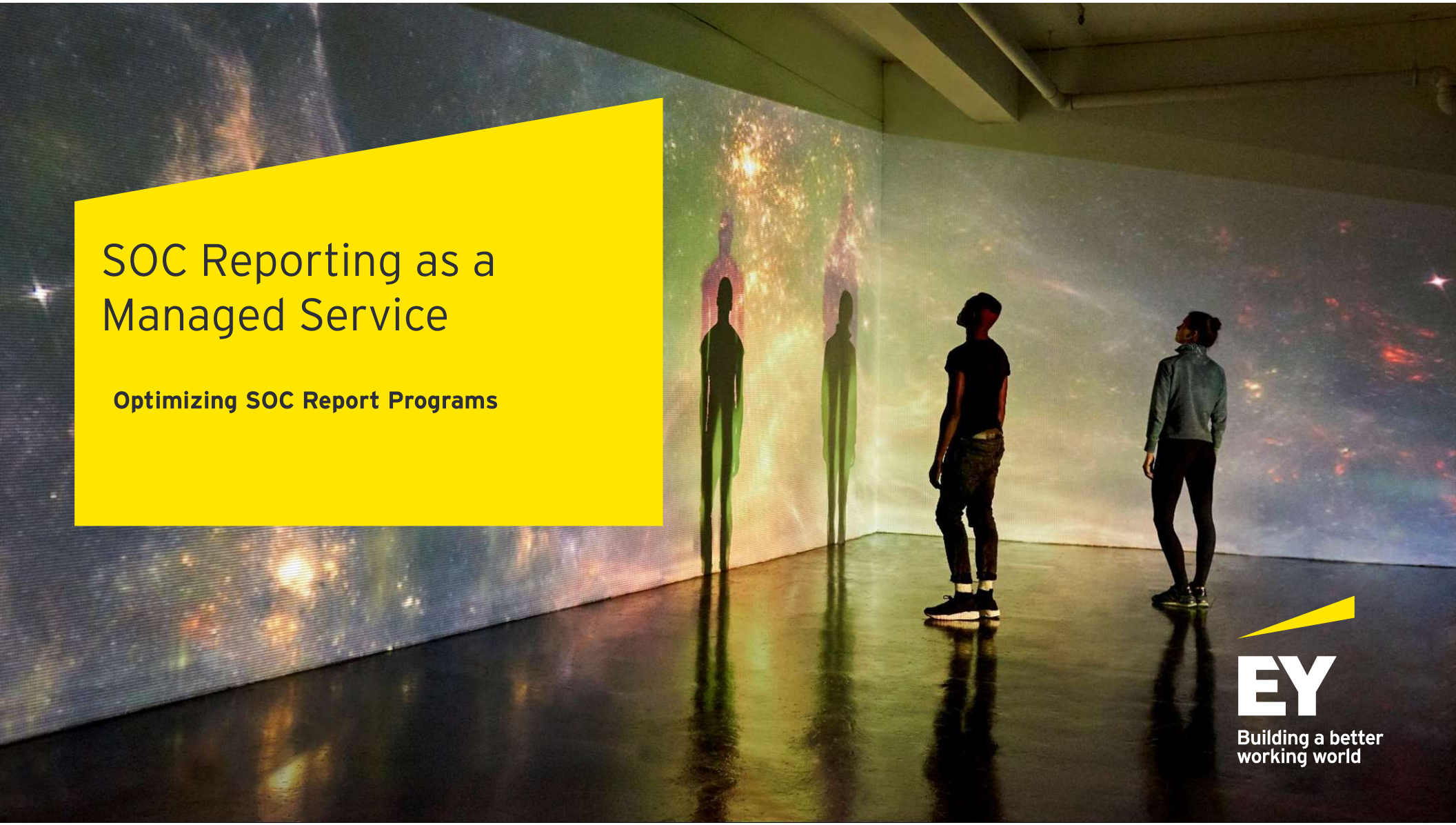
GDPR Assurance Reports:

- Creating trust through transparency, reliability and integrity.

EY

SOC Reporting as a Managed Service

Optimizing SOC Report Programs



EY

Building a better working world

Our collective objectives and discussion topics

Objectives

- Share perspectives of current state customer assurance/compliance programs with technology clients
- Discuss leading practice insights and perspectives related to enhancing customer confidence and trust

Discussion Topics

- Root causes based on experience with other clients
- Leading practices for enhanced compliance and customer assurance programs

EY

Trust is more important than ever

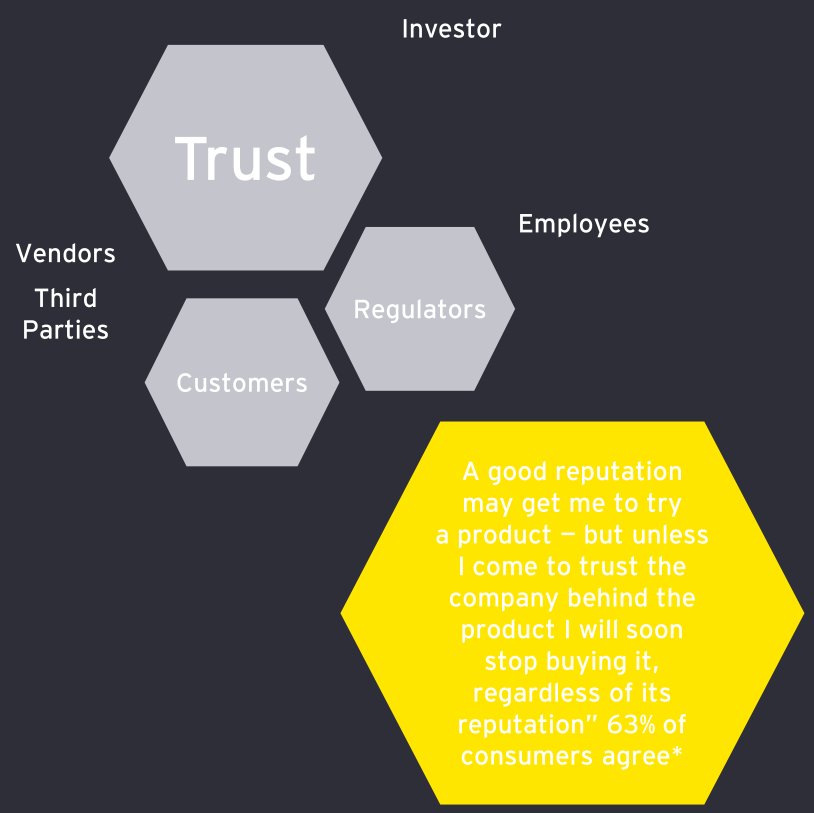
Business today moves at a breath-taking pace: according to a recent study, in 1964 the average life of a company in the S&P 500 was 33 years. That is predicted to drop to 12 years by 2027.

01 https://www.innosight.com/insight/creative-destruction

Trust is the new currency to derive value and loyalty.

Organizations recognize trust is critical to sustaining consumer loyalty and differentiating their brand in the market.

02



EY

Industry trends for Companies with compliance and customer assurance programs

Key Challenges
Customer expectations of sophistication of compliance programs are growing, which is increasing the complexity and resources required to run a compliance program.

1

Lack of Desired Maturity of Compliance Program

Inability to understand compliance related risk for real-time mitigation and decision making

2

Compliance and Audit Inefficiency

Inefficiencies: multiple auditors, reporting periods, sub-service providers, risk and control coverage

3

Lack of Coordination

Risk areas not consistently assigned and tracked to closure

4

Customer Dissatisfaction

Customer question and trust degradation due to multiple audits and control deviations

5

Compliance Cost

Pressure to control and reduce cost of compliance and penalties

6

Risk Awareness

Lack of consistent visibility into compliance risks throughout the organization

EY

Root causes of business impacts based on experience with other clients

Business Impacts

- Stakeholder Dissatisfaction
- Customer and Regulatory Fines
- Program Inefficiencies
- Audit Fatigue

Underlying Root Causes

Governance
Lack of central oversight and decision making

Operating Model
Siloed compliance functions with redundant assessment activities

Contracts
Compliance requirements not consistently considered during the sales pursuit and contracting process

Control Framework
No common view of processes, risks, controls and regulatory requirements

Coordination
Lack of coordination across compliance functions and activities

Issue Management
Lack of timely and sufficient remediation leading to reoccurring and duplicate issues

Compliance Culture
Very reactive with no clear alignment to performance objectives

2nd Line Activities
Varies across groups, often the only time the controls are reviewed are through 3rd line assessments OR 2nd line testing not utilized by 3rd line assessors

Technology
Technology capabilities are under utilized to support compliance activities

EY

Leading practices for enhanced compliance and customer assurance programs

Governance
Integrated Governance
Establish maturity roadmap and determine appropriate governance model across the compliance ecosystem

Operating Model
Op Model Design and Deploy
Definition of desired end-state and transitional op model and operationalization throughout cloud businesses

Contracts
Enhance Customer Enablement
Drive end-to-end awareness of customer assurance processes and enhance efficiency and effectiveness; actively monitor contract provisions and compliance

Control Framework
Program and Control Design
Integrated approach across eco-system, risk-based control rationalization, report optimization, compliance considering standards and frameworks pertinent to LOB

Coordination
Audit PMO and Approach Support Establish program management office to facilitate audit process, track status, and escalate key items to leadership; challenge approach

Issue Management
Formal Issue Mgmt Process
Trusted environment enabling escalation of issues, appropriate risk quantification, and active monitoring of issue remediation. Aligned with retesting by 2nd line

Compliance Culture
Build Culture
Clearly define roles and responsibilities and establish accountability. Invest in training, competency assessment and skills alignment

2nd Line Activities
Control Monitoring and Testing
Build readiness function; shift to greater internal continuous control monitoring and enhance reliance by auditor on internal control testing

Technology
Robotic Process Automation
Establish prioritized automation journey to drive meaningful cost reduction for control execution, evidence generation, control testing, and reporting

EY

Characteristics of a Compliance of the Future Program

Risk-enabled domains

- **Governance and Oversight**
  Governance approvals supported by nimble organizational structure, with flexible (yet well understood) process flows
- **Processes**
  Risk management integrated into the first line of defense maintaining a strong risk oversight while delivering an efficient risk operations model keeping pace with the business landscape
- **People and Capabilities**
  Risk-enabled culture and practices disseminated and shared across the organization with all teams collaborating and understanding their roles
- **Technology and Data**
  Right data from the right and various systems available for quick and informed decisions, feeding into key metrics, automated risk assessments and driving

Characteristics

- **Balanced portfolio designed**
  Evaluating risks across multiple dimensions to monitor what must go right (upside), what could go wrong (downside) and what could surprise you (outside).
- **Real-time Risk Assessment and Monitoring**
  Real time risk assessments to accelerate detection and real-time monitoring of risks (KRIs) to drive agile decision making aligned with strategic priorities
- **Risk informed business decisions**
  Digitizing risk intelligence to enable predictive and real-time reporting to drive agile decision making aligned with strategic priorities
- **SMART Controls**
  Automated and adjustable controls modularly deployed, reusable and supportive of multiple control requirements and adaptive risk profiles,
- **Customer Trust Journey**
  Leverage integrated data to perform ongoing monitoring of customer trust and react to current needs while anticipating future needs
- **Digital mindset and culture to deliver trust**
  Transforming the organization to design a business and risk strategy that is more

EY

The webcast was presented by...

Prince Agarwal

TPRM and Data Privacy Assurance Leader

Senior Manager | Norway

Matt T Beaulieu

Senior Manager Technology Risk

Senior Manager | United States

Dennis Houtekamer

EMEIA SOC Reporting Leader

Associate Partner | The Netherlands