Webinar:
Deep Dive into "Risk", "High Risk" and Risk Assessments in the GDPR

Tuesday, 24 May 2016

11:00 AM US EDT

Centre for Information Policy Leadership
Hunton & Williams LLP

Webinar Agenda

1. Introduction

2. "Risk", "High Risk" and Risk Assessments in the General Data Protection Regulation ("GDPR")

3. Guest Presentations:
   - How you deal with risk in your organisation (e.g. risk methodology, factors which are taken into account during your risk assessment, how do you determine if a processing operation falls within the "risk" or "high risk" category); and
   - Discuss concrete examples on how you approach in the context of (1) data breaches, (2) legitimate interest and (3) data protection impact assessment.

4. Q&A Discussion (*7 Unmute / *6 mute)

Centre for Information Policy Leadership
Hunton & Williams LLP

Speakers

Moderator: Bojana Bellamy
President
Centre for Information Policy Leadership

Hilary Wandall
AVP, Compliance & CPO
Merck & Co., Inc.

Emma Butler
Senior Director, Privacy and Data Protection
RELX Group

Maria Chiara Atzori
Head Data Privacy Switzerland
Novartis

Centre for Information Policy Leadership
Hunton & Williams LLP

Risk-Based Approach in GDPR

Horizontal – Accountability Obligation

- More flexibility for controllers to build, implement and demonstrate privacy programme and compliance measures
- Based on **likelihood and severity of risks for individuals**
- Based on nature, scope, context and purposes of processing

Specific obligations based on risk

- Privacy by design
- Data security
- Security breach notification to DPAs
- Appointment of representative of controller or processor established outside the EU

Specific requirements only for high risk processing

- Security breach notification to individuals
- Data Protection Impact Assessment
- Prior consultation with DPAs for high risk processing that cannot be mitigated

Implied consideration of risk

- Legitimate interest balancing test
- Purpose limitation - determining compatibility of subsequent purposes
- Fair processing

Further guidance provided by DPAs, EDPB, codes of conduct and certifications, DPO

Centre for Information Policy Leadership
Hunton & Williams LLP

Definition of Risk in GDPR

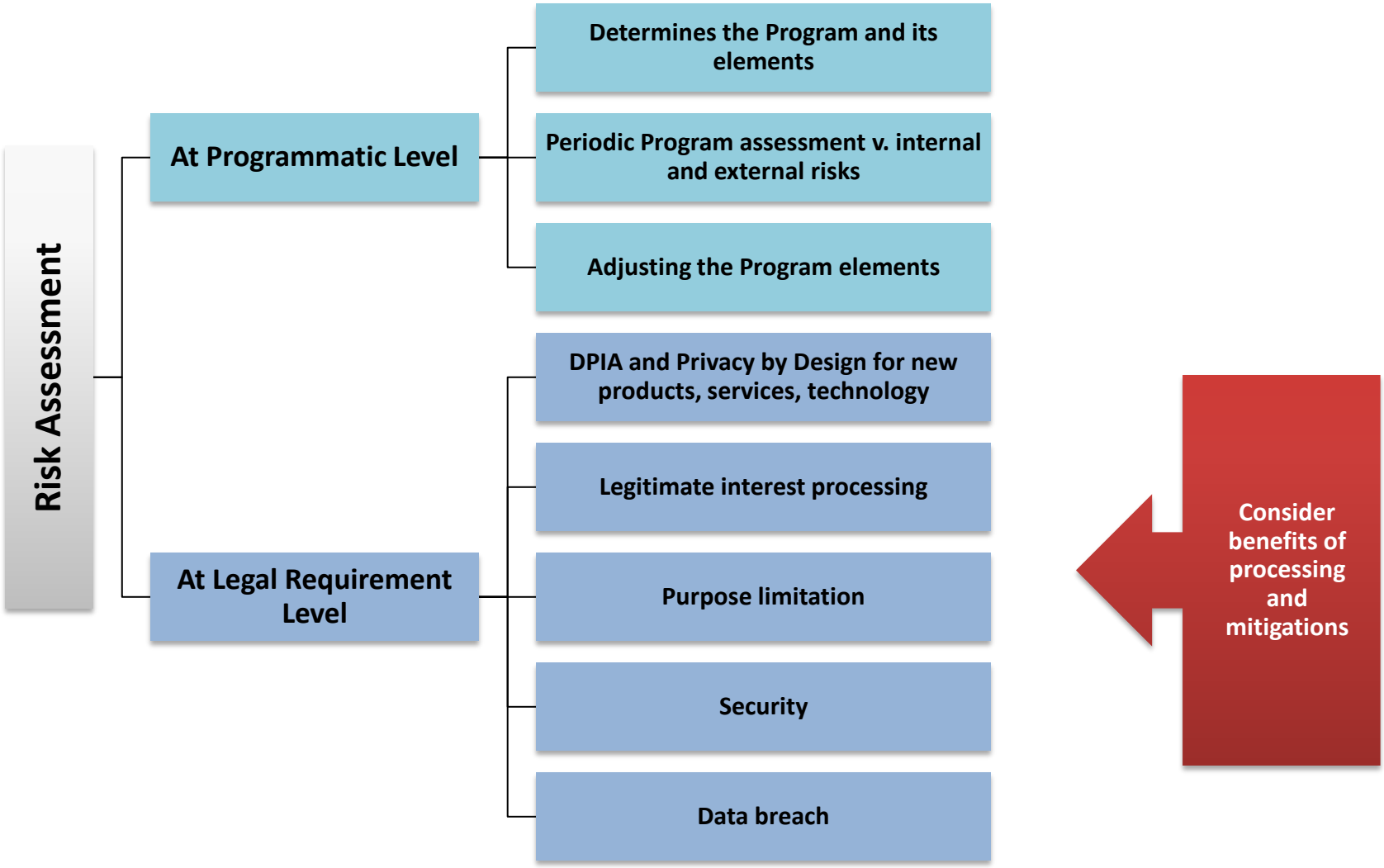
1. Personal data processing that may result in **physical, material or non-material damage**, in particular:
   - Discrimination
   - Identity theft / fraud, financial loss
   - Reputation damage
   - Loss of confidentiality of personal data protected by professional secrecy
   - Unauthorised reversal of pseudonymisation
   - Any other significant economic or social disadvantage
   - Individuals deprived of rights and freedoms, or prevented from exercising control over their data
   - Processing sensitive data, including genetic data
   - Profiling (personal aspects are evaluated (e.g. analyse or predict work performance, economic situation, health, personal preferences, behaviour, location) to create or use personal profiles
   - Processing children's and vulnerable persons' data
   - Processing large amounts of data and individuals

2. High risk

- High likelihood or severity of risks above, or involve use of new technology, or no DPIA carried out before, or time elapsed since initial processing

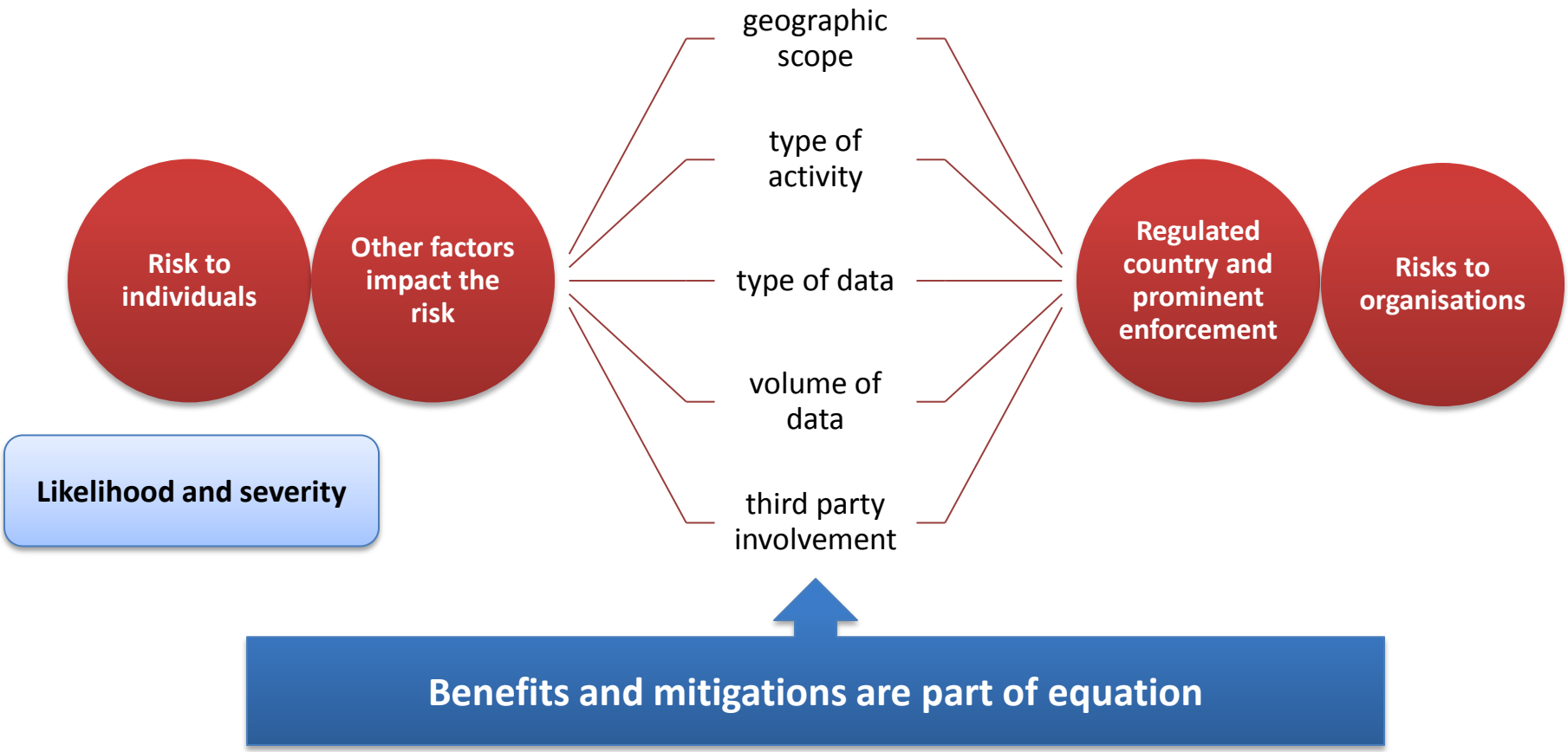
- Pre-defined types of high-risk processing – automated decision taking; large scale processing of sensitive data or criminal convictions; systematic monitoring of public areas

Detailed View of Risk Assessments in the Context of Organisational Privacy Compliance Programs



The Risk Assessment Process – Incorporating Risks, Benefits, Mitigations

Risk determines privacy program, its elements, levels of requirements and applied controls



Benefits and mitigations are part of equation

Centre for Information Policy Leadership
Hunton & Williams LLP

Guest Speaker

Hilary Wandall

AVP, Compliance & CPO

Merck & Co., Inc.

MSD

Centre for Information Policy Leadership
Hunton & Williams LLP

Our Approach…

Our global Privacy Program supports our company mission of saving and improving lives by promoting and assuring a culture of privacy accountability where four privacy values are embedded into the way we work and how we engage people everywhere we operate

Respect	*Trust*	*Prevent Harm*	*Comply*
We recognize that privacy concerns often relate to the essence of who we are, how we view the world, and how we define ourselves, so we strive to respect the perspectives and interests of individuals and communities and to ***be fair*** and transparent in how we use and share information about them	We know that trust is vital to our success, so we strive to build and preserve the trust of our customers, employees, patients and other stakeholders in how we respect privacy and protect information about people	We understand that misuse of information can create both tangible and intangible harms for individuals, so ***we seek to prevent physical, financial, reputational, and other types of privacy harms to individuals***	We have learned that laws and regulations cannot always keep pace with rapid changes in technologies, data flows, and ***associated shifts in privacy risk and expectations***, so we strive to comply with both the spirit and the letter of privacy laws in a manner that drives consistency and efficiency for our global business operations

MSD

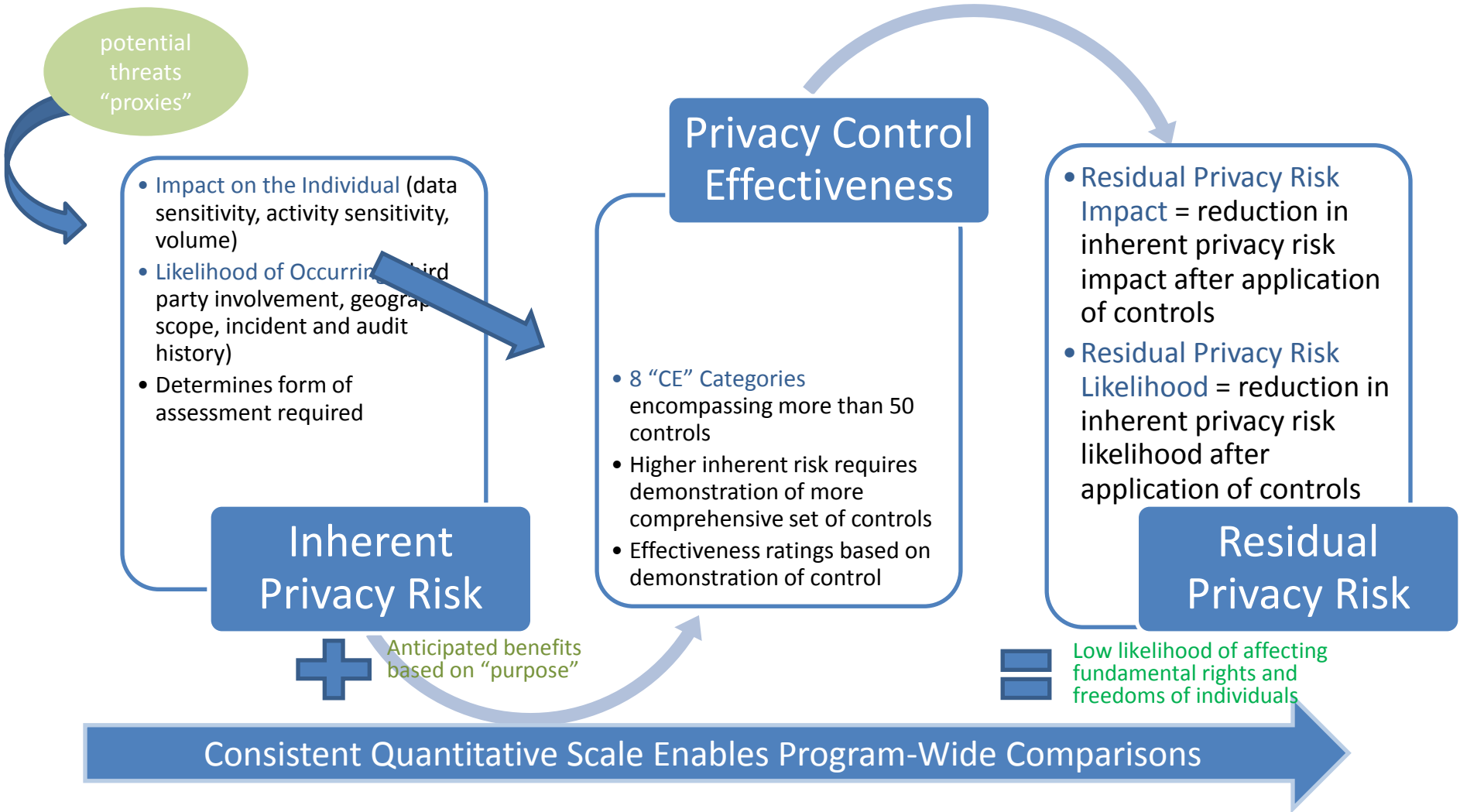
Centre for Information Policy Leadership
Hunton & Williams LLP

Our Risk Practices

Merck & Co., Inc. (MSD) Risk Management Practice	Alignment to GDPR
Process-level risk evaluation (*Respect, Prevent Harm)*	
Privacy impact assessment • Inherent risk and benefit determination during scope/threshold analysis (*Fairness principle)* • Control effectiveness analysis • Residual risk analysis	Article 25 Article 35 Article 36
Scientific research • Ethics committee/IRB waiver of consent for minimal risk	Article 9 Article 89
Breach notification • Where not expressly required by law, where risk of harm warrants notification, or, as applicable (e.g., HIPAA) where risk assessment shows greater than low probability of data compromise	Article 33
Program-wide risk evaluation *(Comply)*	
External factors (e.g., laws, policy trends) analyzed by mapping to applicable control effectiveness categories	Article 24

Centre for Information Policy Leadership
Hunton & Williams LLP

Privacy Risk in Practice



MSD

Centre for Information Policy Leadership
Hunton & Williams LLP

Application – 2 Projects

Threshold Scope Analysis – Inherent Privacy Risk

Consumer Health App

Risk Factor	Analysis	Risk Level
Data	Sensitive	High
Activity/Context	Sensitive	High
Data Volume	> 10,000 users	Medium
Data Subjects	Consumers	Medium
Third Parties	Yes, Multiple – In country	Medium
Third Countries	Other Region	High
Applicable Law	Yes – Recent Enforcement	High
Incident History	1 Instance	Medium
Overall Assessment		Medium-High

Employee Expense App

Risk Factor	Analysis	Risk Level
Data	Confidential	Medium
Activity/Context	Confidential	Medium
Data Volume	Pilot (<1,000)	Low
Data Subjects	Employees	Medium
Third Parties	No	Low
Third Countries	No	Low
Applicable Law	Yes – Past Enforcement	Medium-High
Incident History	No	Low
Overall Assessment		Medium

Likelihood Factors -- Impact Factors

Impact Factors – Likelihood Factors

MSD

Application – 2 Projects

Applying Inherent Privacy Risk Analysis to Controls Assessment

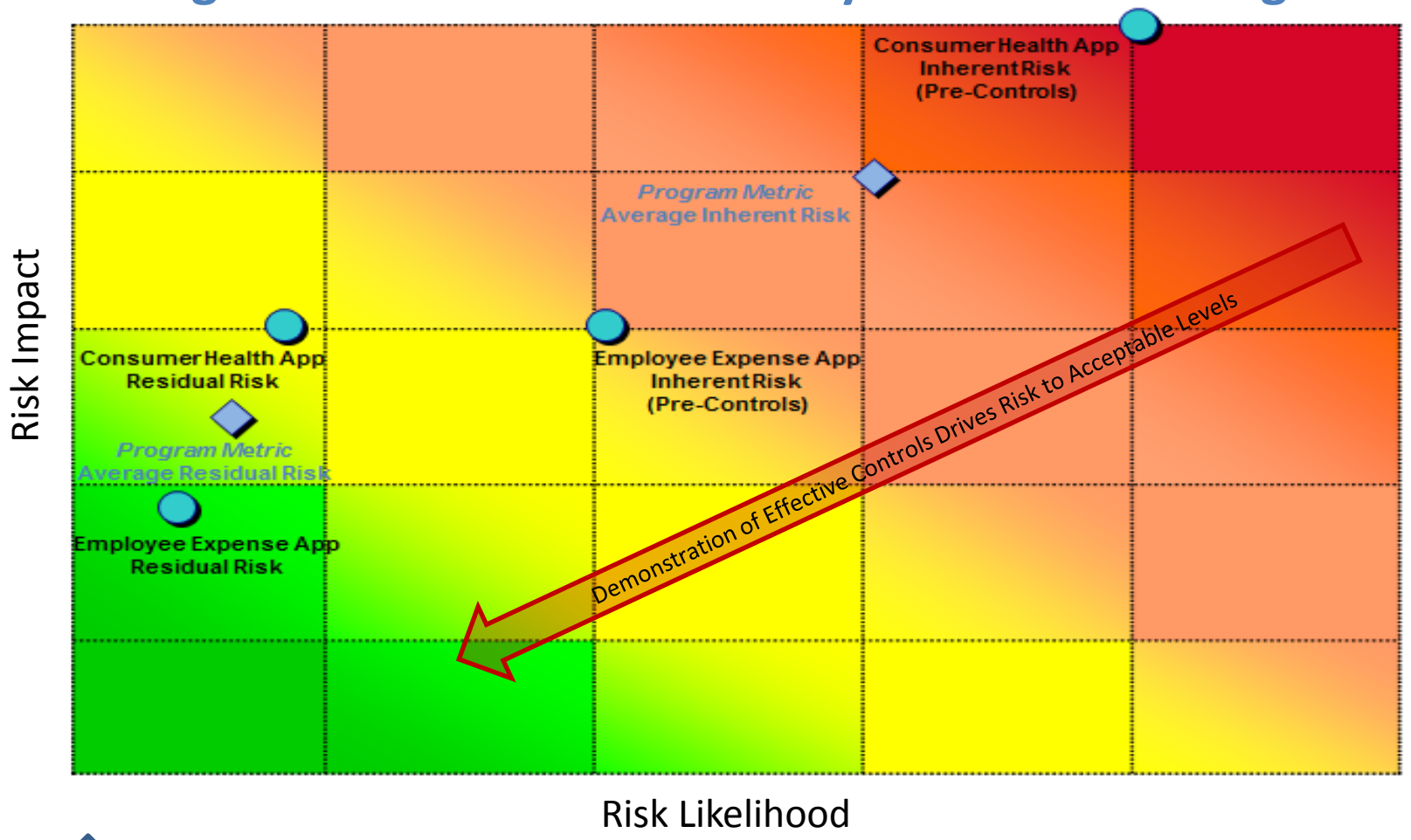
Assessment Criteria	Consumer Health App	Employee Expense App
Personnel Expertise	Expert (Privacy Office)	Advanced (Steward w/ Privacy Office)
Assessment Documentation	Global Privacy System	Local Inventory and Records
In Scope of Annual Management Certification	Yes (Functional Leader)	Yes (Country Leader)
Evidence	Yes, in Global Privacy System	Yes, in Local Records
Transparency Analysis	Yes	Yes
Governance Analysis	Yes	Yes
Individual Rights Analysis	Yes	Yes
Security Analysis	Yes	Yes
Incident Management Analysis	Enhanced	Yes
Third Party Analysis	Yes	No
More Stringent Local Law Analysis	Yes	No
Online Privacy Certification/Seal	Yes	No

6 of 8 Control Effectiveness Categories

Centre for Information Policy Leadership
Hunton & Williams LLP

Comparing 2 Projects

Evaluating the Effectiveness of Privacy Controls and Program Risk



Standard Quantitative Measures Enable Program-Wide Averages and Trending

MSD

Centre for Information Policy Leadership
Hunton & Williams LLP

Guest Speaker

Emma Butler

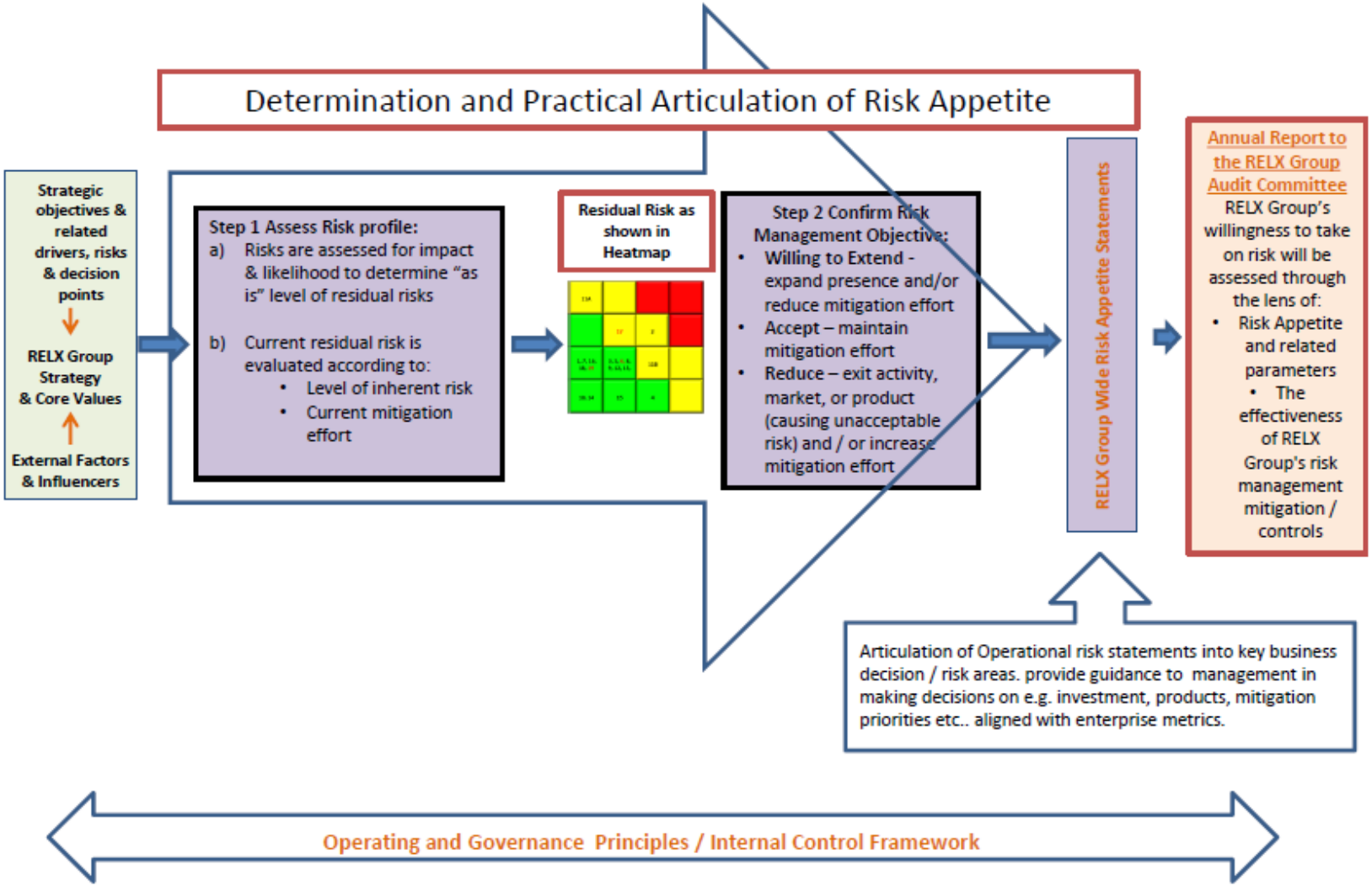
Senior Director, Privacy and Data Protection

RELX Group

Centre for Information Policy Leadership
Hunton & Williams LLP

Determination and Practical Articulation of Risk Appetite

Confidential, for internal use only

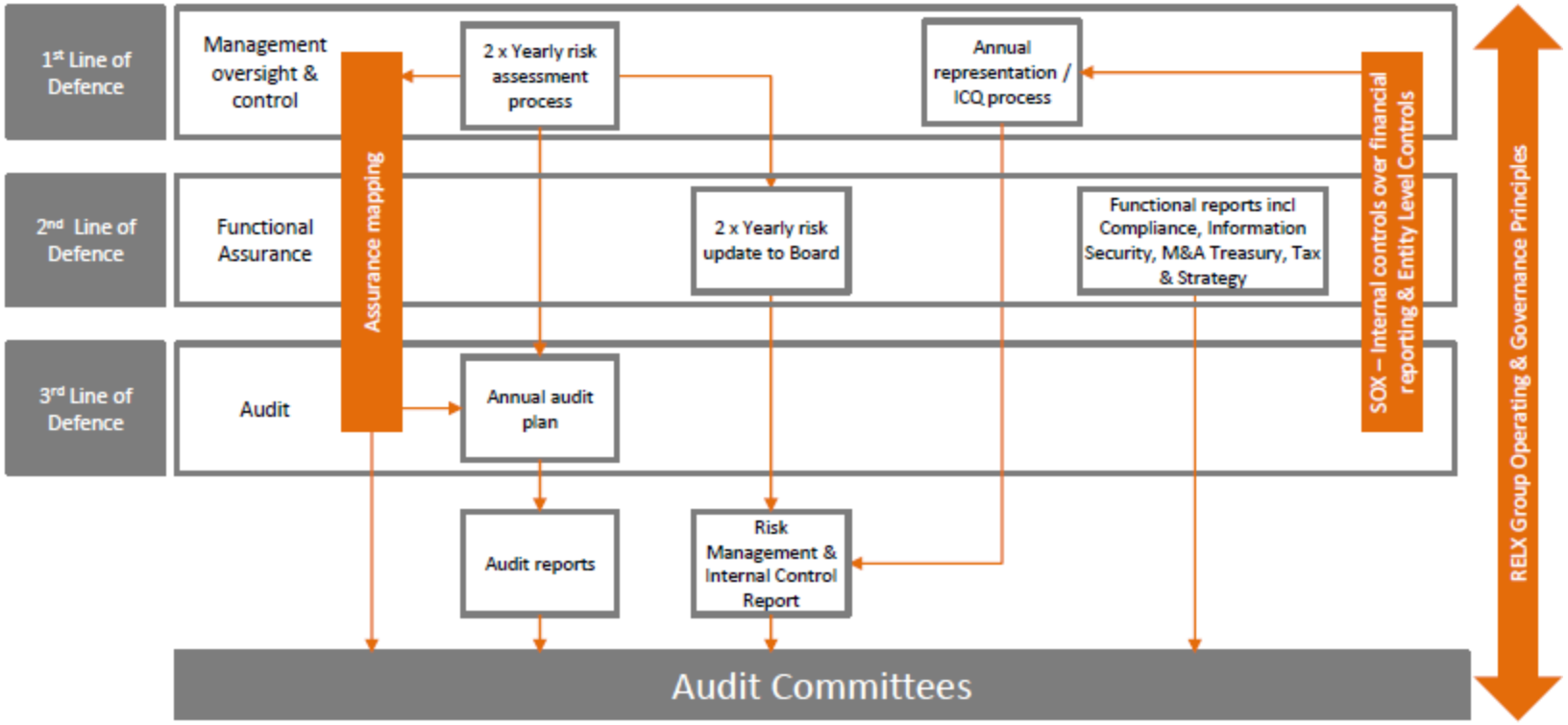


Centre for Information Policy Leadership
Hunton & Williams LLP

Risk Management and Internal Control Framework

Confidential, for internal use only

RELX Group's Risk Management and Internal Control Framework – Three Lines of Defence



Centre for Information Policy Leadership
Hunton & Williams LLP

Practical Examples

Practical example: legitimate interests

- Article 29 opinion WP 217
- Are the interests legitimate? Company (sometimes customer interests); individuals.
- Is the processing necessary to achieve the interests pursued?
- Do the rights of the individual override company interests?
- Are there safeguards we can put in place? Data minimisation, technical and organisational measures, privacy by design, transparency…
- Assessment also covers: broader societal impacts; benefits to individuals / society; risks of not doing the processing.

Practical example: data protection impact assessments

- Data types: some flagged as needing more attention.
- Assessment against 8 UK DP Act principles.
- Considers: fairness (transparency); fairness (proportionality and reasonable expectations of consumers).
- Risks identified that could lead to questions about compliance with a particular principle.
- Risks and mitigation factors / solutions granular and specific to project.

Centre for Information Policy Leadership
Hunton & Williams LLP

Guest Speaker

Maria Chiara Atzori

Head Data Privacy Switzerland

Novartis

Privacy Risk Assessment at Novartis

Maria Chiara Atzori, Head Data Privacy Switzerland

Basel, 24 May 2016

NOVARTIS

Robust approach to increase control while reducing bureaucracy and combining different assessments

From:

Different Privacy Assessments

Swiss Privacy Inventory

- 30 questions (Online questionnaire)

Privacy Impact Assessment (PIA)

- 80+ questions (Word document)

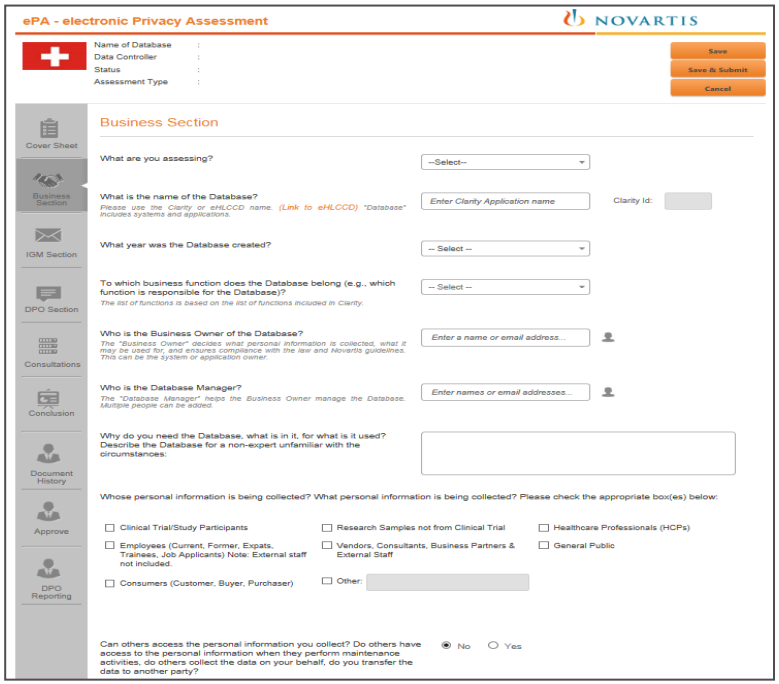
Business Impact Assessment (BIA)

- 28 privacy questions (Excel spreadsheet)

To:

One user friendly tool

- 12 questions for the Business Owner
- 6 questions for Information Manager



NOVARTIS

Novartis current privacy risk assessment towards its further evolution

Classification of risk

- Need to review the distinction between risk and high risk processing of data
- Increase focus on likelihood and severity of the risk to the individuals

Balancing risks

- Need to improve understanding of data privacy risks and its implications in the context of business initiatives
- Absence of an assessment of the processing benefits

Mitigation options

- Not context related and not sector-specific
- Unilateral mitigation of risks
- Establish new set of safeguards to achieve strong protection

GDPR opened gaps

- Consultation of DPAs for high risk processing
- Legitimate interest balancing
- Purpose limitation (e.g. secondary use of data)

Develop a sound privacy risk assessment to build trust and confidence

Be able to solve the tension between data availability and harm to individual

- Identification of gaps between industry and patients' interests and potentially threatening activities in public perception
- Sound assessment of privacy risk and fit for purpose mitigation of gaps

Build trust and confidence

- Future use cases (e.g., RWE) depend on patients entrusting industry with personal data and content for far reach analyze
- Sound privacy risk assessment as a cornestone of accountability

Centre for Information Policy Leadership
Hunton & Williams LLP

Q&A Discussion

If you would like to ask a question, please hit *7 (star 7) to unmute your phone.

Please hit *6 (star 6) to mute your phone again.

Bojana Bellamy
President
Centre for Information Policy Leadership

Emma Butler
Senior Director, Privacy and Data Protection
RELX Group

Hilary Wandall
AVP, Compliance and CPO
Merck & Co., Inc.

Maria Chiara Atzori
Head Data Privacy Switzerland
Novartis

Centre for Information Policy Leadership
Hunton & Williams LLP

Contacts

Bojana Bellamy
President
Centre for Information Policy Leadership
bbellamy@hunton.com

Emma Butler
Senior Director, Privacy and Data Protection
RELX Group
emma.butler@relx.com

Hilary Wandall
AVP, Compliance and CPO
Merck & Co., Inc.
hilary.wandall@merck.com

Maria Chiara Atzori
Head Data Privacy Switzerland
Novartis International
maria_chiara.atzori@novartis.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton & Williams Privacy and Information Security Law Blog
www.huntonprivacyblog.com

LinkedIn **FOLLOW US ON**
linkedin.com/company/centre-for-information-policy-leadership

FOLLOW US ON TWITTER
@THE_CIPL