Risk assessments and applying organisational controls for GDPR compliance

Presented by:
• Alan Calder, founder and executive chairman, IT Governance

2 November 2017
Introduction

• Alan Calder
• Founder of IT Governance
• The single source for IT governance, cyber risk management and IT compliance
• [www.itgovernance.co.uk](http://www.itgovernance.co.uk)
IT Governance Ltd: GRC one-stop shop

IT governance, risk and compliance

Cyber resilience

Governance and risk management

- Information security and ISO 27001
- Business continuity management and ISO 22301
- PCI DSS
- Penetration testing
- Data protection
- Incident response management
- Change management
- IT governance
- Service management
- Project management
- ITIL® and ISO 20000
- COBIT®
- PRINCE2® and PMBOK®
- Consultancy and certification
- Security testing
- Training and qualifications
- Software tools
- Toolkits and publications

All verticals, sectors and all organisational sizes
Agenda

• An overview of the General Data Protection Regulation (GDPR) and risk assessments.
• The process for risk management and industry best practice for risk treatment.
• The components of an internal control system and privacy compliance framework.
• ISO 31000 principles and the risk management process.
The GDPR’s impact

- UK organisations that process personal data only have a short time to make sure that they are compliant.
- The Regulation extends the data rights of individuals, and requires organisations to develop clear policies and procedures to protect personal data, and adopt appropriate technical and organisational measures.

“This Regulation shall be binding in its entirety and directly applicable in all Member States.”

8 April 2016
Council of the European Union adopted the GDPR

12 April 2016
The GDPR was adopted by the European Parliament

4 May 2016
The official text of the Regulation was published in the Official Journal of the EU

24 May 2016
The Regulation entered into force

25 May 2018
The GDPR will apply

Material and territorial scope

Natural person = a living individual

- Natural persons have rights associated with:
  - The protection of personal data;
  - The processing of personal data; and
  - The unrestricted movement of personal data within the EU.

In material scope:
- Personal data that is processed wholly or partly by automated means.
- Personal data that is part of a filing system, or intended to be.

The Regulation applies to controllers and processors in the EU, irrespective of where processing takes place.

It applies to controllers outside the EU that provide services into the EU.
Penalties

Administrative fines

- Administrative fines will, in each case, be effective, proportionate and dissuasive, and take account of the technical and organisational measures that have been implemented.

€10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year.

€20,000,000 or, in the case of an undertaking, up to 4% of the total worldwide annual turnover in the preceding financial year.
The GDPR and risk management frameworks

• **Article 32:** “The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.”

• “In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.”

• “Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.” (Article 24-1)

The data protection officer (DPO) plays a key bridging role between corporate risk management, broader cyber security risk management and managing risks to personal data.

Article 35: Where processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

- A data protection impact assessment (DPIA) is particularly required in the case of:
  - Automated processing, including profiling, and on which decisions are based that produce legal effects concerning natural persons;
  - Large-scale processing of special categories of data or of personal data relating to criminal convictions; and
  - A systematic monitoring of a publicly accessible area on a large scale.
A DPIA will set out as a minimum:

- A systematic description of the processing and purposes.
- Legitimate interests (where applicable) pursued by the controller.
- An assessment of the necessity and proportionality of the processing.
- An assessment of the risks to the rights and freedoms of the data subjects.
- **The measures envisaged to address the risks, including:**
  - Compliance with approved codes of conduct should be taken into account.
  - All safeguards and security measures to protect data and to demonstrate compliance.
- Where appropriate, consult the data subjects.
What is risk?

- The effect of uncertainty on objectives (ISO 31000, etc.).
- A combination of the likelihood of an incident occurring and the impact, if it does occur, on the organisation.
- A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action (businessdictionary.com).
- Risk can be good or bad.
Key definitions

**Risk management:** the coordinated activities to direct and control an organisation with regard to risk.

**Risk assessments:** the overall process of risk identification, risk analysis and risk evaluation.

**Risk treatment:** the process to modify risk.
Risk and what it means under the GDPR

Risks to individuals: the potential for damage or distress.

Risks to organisations: financial and/or reputational impact of a data breach.

Privacy risk should already be on the CORPORATE RISK REGISTER
Risk assessments

Risk assessments help:

- Identify the threats that could harm and affect an organisation’s assets;
- Determine the value and sensitivity of data by identifying the level of risk that data carries if threatened; and
- Implement cost-effective measures to mitigate and reduce the risk.
Risk assessments determine the appropriate controls to reach acceptable levels of risk.

Risk cannot exist without these three components:

1. An asset that has value and requires protection.
2. A threat that can hurt it.
3. A vulnerability – a weakness that allows the threat to reach the asset.
Why do we assess risk?

A risk assessment informs a proper balance of safeguards against the risk of failing to meet business objectives.

Inform a position so that:
• Removal of safeguards will increase the risk of loss to an unacceptable level; and
• Adding any safeguards would make the security system too expensive/bureaucratic.

... and therefore it is a means by which expenditure on security and contingency can be justified.
Examples of risk

Data that is:

- **Inaccurate**, insufficient or out-of-date
- **Kept** for too long
- **Excessive** or irrelevant
- **Disclosed** to the wrong people
- **Insecurely** transmitted/stored
- **Used in ways that are unacceptable or unexpected**
Risk assessment (based on ISO 31000)

Identify risks

- Workshop, facilitated by a risk expert
- (Key) Assets at risk
- (Key) Threat – vulnerability relationships
- NB: ‘vulnerability’: weakness of an asset or control that can be exploited by one or more threats

Analyse risks

- Consequence (impact)
- Probability (likelihood)
- Level of risk (e.g. impact x likelihood)

Evaluate risks

- Compare risks with risk criteria (e.g. risk appetite)
Risk criteria – per ISO 31000

• **When defining risk criteria, consider:**
  - The nature and types of causes and consequences that can occur and how they will be measured;
  - How likelihood will be defined;
  - The timeframe(s) of the likelihood and/or consequence(s);
  - How the level of risk is to be determined;
  - The views of stakeholders;
  - The level at which risk becomes acceptable or tolerable; and
  - Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

Risk scenarios – components

Adapted from ISACA, The Risk IT Framework, USA, 2009

**Threat type**
- Malicious
- Accidental/error
- Failure
- Natural
- External requirement

**Actor**
- Internal (staff, contractor)
- External (competitor, outsider, business partner, regulator, market)

**Event**
- Disclosure
- Interruption
- Modification
- Theft
- Destruction
- Ineffective design
- Ineffective execution
- Rules and regulations
- Inappropriate use

**Asset/resource**
- People & organisation
- Process
- Infrastructure (facilities)
- IT Infrastructure
- Information
- Applications

**Time**
- Duration
- Timing of occurrence (critical, non-critical)
- Timing to detect
ISO 27005 – risk management

Risk communication and consultation

Context establishment

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Risk decision point 1
Assessment satisfactory?

Risk decision point 2
Treatment satisfactory?

Risk acceptance

Risk monitoring and review
Risk and countermeasures

**Likelihood**
- Low
- Medium
- High
- Very low
- Low
- Medium
- High

**Negative impact**
- High
- Medium
- Low
- Very high
- High
- Medium
- Low

Copyright IT Governance Ltd 2017 – v1.1
• ISO 27001 information security management system (ISMS) controls are typically selected by objective, taking into account:
  - National and international legislation and regulations and baseline security criteria;
  - Organisational objectives;
  - Operational requirements and constraints;
  - Cost of implementation and operation (versus risks being reduced and proportional to the organisation);
  - That they should be implemented to monitor, evaluate and improve the efficiency and effectiveness of information security controls to support the organisation’s aims; and
  - Balancing investment against harm from security failures.
Example countermeasures

People
- Security training and awareness
- Staff vetting
- Leaver management

Process
- System admin controls
- Financial accounting
- Business continuity planning
- Reporting and reacting to incidents
- Media controls

Product/technology
- Site/building physical security
- Bomb detection
- Fire/power outage protection
- Identification and authentication
- Logical access control
- Software change control
Examples of risk treatment

- **Reduce** data collected
- **Retention** policy
- **Secure destruction** of information
- **Access** control
- **Training** and awareness
- **Pseudonymise** information
- **Contracts** or data-sharing agreements
- **Acceptable use** policy
- **Subject access** request process
- **External supplier risk** assessments
Assess the costs and benefits

Cost

Risk acceptance

Number of controls

Controls implemented

Vulnerabilities

Copyright IT Governance Ltd 2017 – v1.1
Next steps

A practical approach to risk management for GDPR compliance:

• Agree approach to risk management.
• Degree of assurance required.
• Conduct risk assessment:
  – Ensure those involved understand the methodology (training?) to ensure comparable and reproducible results.
• Manage (reduce) risk to level of assurance required using controls and compare to standards such as ISO 30001 or ISO 27001.
Next steps

A practical approach to risk management for GDPR compliance

Step 1:
- Assess risk
- Identify risk
- Prioritise initiatives
Next steps

A practical approach to risk management for GDPR compliance

Step 2:

Classify data

Take action

Implement incident management response
Next steps

A practical approach to risk management for GDPR compliance

Step 3: Demonstrate ongoing risk and incident monitoring
Risk assessment tool: vsRisk™

- **Simplification**: minimises the manual hassle and complexity of carrying out an information security risk assessment, saving time and resources.
- **Replication**: risk assessments can be repeated easily in a standard format year after year.
- **Generates reports**: for exporting, editing and sharing across the business and with auditors.
- **Automation**: the fast and simple way to carry out a risk assessment.
IT Governance: GDPR one-stop shop

Self-help materials

A pocket guide
www.itgovernance.co.uk/shop/Product/eu-gdpr-a-pocket-guide

Implementation manual
www.itgovernance.co.uk/shop/Product/eu-general-data-protection-regulation-gdpr-an-implementation-and-compliance-guide

Documentation toolkit
www.itgovernance.co.uk/shop/Product/eu-general-data-protection-regulation-gdpr-documentation-toolkit

Compliance gap assessment tool
www.itgovernance.co.uk/shop/Product/eu-gdpr-compliance-gap-assessment-tool
Training courses

One-day accredited Foundation course (classroom, online, distance learning)
www.itgovernance.co.uk/shop/Product/certified-eu-general-data-protection-regulation-foundation-gdpr-training-course

Four-day accredited Practitioner course (classroom, online, distance learning)
www.itgovernance.co.uk/shop/Product/certified-eu-general-data-protection-regulation-practitioner-gdpr-training-course

One-day DPIA workshop (classroom)
www.itgovernance.co.uk/shop/Product/data-protection-impact-assessment-dпia-workshop
IT Governance: GDPR one-stop shop

GDPR consultancy

- **Gap analysis**
  Our experienced data protection consultants can assess the exact standing of your current legal situation, security practices and operating procedures in relation to the Data Protection Act (DPA) or the GDPR.

- **Data flow audit**
  Data mapping involves plotting all of your data flows, drawing up an extensive inventory of the data to understand where the data flows from, within and to. This type of analysis is a key requirement of the GDPR.

- **DPO as a service**
  Outsourcing the DPO role can help your organisation address the compliance demands of the GDPR while staying focused on its core business activities.

- **Implementing a personal information management system (PIMS)**
  Establishing a PIMS as part of your overall business management system will make sure that data protection management is placed within a robust framework, which will be looked upon favourably by the regulator when it comes to DPA compliance.

- **Implementing an ISMS compliant with ISO 27001**
  We offer flexible and cost-effective consultancy packages, and a comprehensive range of bespoke ISO 27001 consultancy services, that will help you implement an ISO 27001-compliant ISMS quickly and without hassle, no matter where your business is located.

- **Cyber Health Check**
  The two-day Cyber Health Check combines on-site consultancy and audit with remote vulnerability assessments to assess your cyber risk exposure.
Questions?