IBM Security technology and services for GDPR programs

GIULIA CALIARI – SECURITY ARCHITECT
Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation.

Clients are solely responsibility for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability.

IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.
Information Security and Data Privacy are correlated but different and must be managed accurately

Information Security and Data Privacy: differences and interactions

**Information Security**

Information security is **all of the practices and processes that are in place to ensure data is not being accessed or used by unauthorized individuals or parties**. It covers a wider array of data than personal data, because it includes the protection of all the information and asset managed for the business.

Organizational, Technical and Physical Controls; mostly as per Industry Standards (ISO 27001).

Some Examples:

- Information Security Policy
- Security Risk analysis, Security Risk Treatment Plan, Information Security Appropriate organizational and technological Measure
- Security Incidence Response Plan
- IAM (Identity and Access Management)
- SIEM (Security Incident and Event Management)
- Data Security
- Firewalls
- Encryption
- Locks, guards, video surveillance

**Data Privacy**

Data privacy is concerned with **establishing rules that govern the collection and handling of personal information**. Handling personal data includes processing, use, transfer, sharing and deletion.

- Privacy Strategy Policy
- Privacy Risk Analysis, Privacy Risk Treatment Plan: Privacy appropriate organizational and technological Privacy Measure
- Privacy Treatment registrations
- Collection Minimization, Transparency
- Notice, Choice, Consent
- Purpose Specification, Use Limitation
- Data Security
- Access, Rectification and Erasure … Rights of Data Subjects
- Retention Periods
- 3rd Party Vendor Requirements
- Cross-border Export Restrictions
- Cross-border Access Restrictions
- Data Breach Notification
- Accountability
IBM’s GDPR approach is holistic

IBM has clustered GDPR activities across three domains:

1. **Privacy Compliance Management System**, to address overall Privacy Accountability covering Privacy strategy and risk and compliance, Privacy Stakeholder identification, PDCA Process, Privacy Documentation and evidence management.

2. **Privacy Enforcement**, starts from Data Discovery based on Privacy Risk Analysis, to address the identification, design, development, implementation, management and documentation collection of appropriate Privacy Measures and Privacy Specific fulfilments (Notice, Consent, Personal Data Management, Data Subject Rights Management, etc.) covering also application and ICT Data Management aspects.

3. **Security Enforcement**, based on Security Risk Analysis, to address the identification, design, development, implementation, management and documentation collection of adequate Security Measures and Security Specific fulfilment (Data Security, Data Breach, Cryptography, etc.)
IBM approach to meet GDPR requirements is structured across five phases

**Assess**
- IBM GDPR Readiness Assessment
  - Identify GDPR impact and plan Technical and Organizational Measures (TOM)

**Design**
- Defined implementation plan
  - Includes Data Protection controls, processes and solutions to be implemented.

**Transform**
- Process enhancements completed
  - TOMs in place: Personal Data discovery, classification and governance in place

**Operate**
- Operational framework in place
  - Begin the new way of working

**Conform**
- Ongoing monitoring and reporting
  - Monitor TOMs execution to deliver results to internal and external stakeholders

---

**Privacy Compliance Management System**
- Training, processes, and tools
- Deliver GDPR
- Monitor security and privacy using TOMs
- Evaluate adherence to GDPR standards

**Privacy Enforcement**
- Privacy by Design, Security by Design

**Security Enforcement**
- Management and Security

---

**Assessments and roadmap**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Activity**
- Assessments and roadmap
- Design
- Transform
- Operate
- Conform

---

**Outcome**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Phase**
- Assess
- Design
- Transform
- Operate
- Conform

---

**IBM GDPR**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Assessments**
- Identify GDPR impact and plan Technical and Organizational Measures (TOM)

---

**Design**
- Defined implementation plan
  - Includes Data Protection controls, processes and solutions to be implemented.

---

**Operate**
- Operational framework in place
  - Begin the new way of working

---

**Conform**
- Ongoing monitoring and reporting
  - Monitor TOMs execution to deliver results to internal and external stakeholders

---

**Privacy Compliance Management System**
- Training, processes, and tools
- Deliver GDPR
- Monitor security and privacy using TOMs
- Evaluate adherence to GDPR standards

---

**Privacy Enforcement**
- Privacy by Design, Security by Design

---

**Security Enforcement**
- Management and Security

---

**Assessments and roadmap**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Activity**
- Assessments and roadmap
- Design
- Transform
- Operate
- Conform

---

**Outcome**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Phase**
- Assess
- Design
- Transform
- Operate
- Conform

---

**IBM GDPR**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Assessments**
- Identify GDPR impact and plan Technical and Organizational Measures (TOM)

---

**Design**
- Defined implementation plan
  - Includes Data Protection controls, processes and solutions to be implemented.

---

**Operate**
- Operational framework in place
  - Begin the new way of working

---

**Conform**
- Ongoing monitoring and reporting
  - Monitor TOMs execution to deliver results to internal and external stakeholders

---

**Privacy Compliance Management System**
- Training, processes, and tools
- Deliver GDPR
- Monitor security and privacy using TOMs
- Evaluate adherence to GDPR standards

---

**Privacy Enforcement**
- Privacy by Design, Security by Design

---

**Security Enforcement**
- Management and Security

---

**Assessments and roadmap**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Activity**
- Assessments and roadmap
- Design
- Transform
- Operate
- Conform

---

**Outcome**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Phase**
- Assess
- Design
- Transform
- Operate
- Conform

---

**IBM GDPR**
- IBM GDPR Readiness Assessment
- IBM GDPR Security Assessment

---

**Assessments**
- Identify GDPR impact and plan Technical and Organizational Measures (TOM)

---

**Design**
- Defined implementation plan
  - Includes Data Protection controls, processes and solutions to be implemented.

---

**Operate**
- Operational framework in place
  - Begin the new way of working

---

**Conform**
- Ongoing monitoring and reporting
  - Monitor TOMs execution to deliver results to internal and external stakeholders

---
IBM Security technology supporting customers in their GDPR journey

Security & Traceability

- Monitor and audit access to personal data, detection and alerting of non-authorized access
- Fine-grained control of data modification

Incident Management

- Identification of attack and potential data breaches
- Monitor & audit of the overall infrastructure

Purposes for GDPR

Focus on Software

- Incident response following a suspected or actual breach
- Orchestration of incident response processes including collection of forensic information, analysis, reporting and remediation

IBM Security technology

Guardium
Radar
Resilient
AppScan
IBM Security
IAM
XGS
MaaS360
BIGFIX
Security & Traceability – Guardium for GDPR

Fine grained data access control

IBM Security

1. Identify and Mitigate Security Vulnerabilities
2. Discover & Classify Personal Data
3. Monitor and track data access and modification
3. Enforce right to access, modify,.. data
3. Compliance Reporting
4. Encrypt/Obfuscate (Pseudonimize)

Discover and classify data, assess vulnerabilities, report on entitlements
Monitor data and file activity
Block, mask, alert, and quarantine dynamically
Encrypt, mask, and redact sensitive data
Automate compliance and auditing
ANALYTICS
Guardium Data Activity Monitor (DAM) for Data
Beyond monitoring and auditing

Identify and respond to detected outliers with a convenient graphical interface

- Anomaly hours flagged red or yellow
- Click bubble for Outlier view

Detect symptoms that may indicate database attacks

Identify Stored Procedures that may hide malicious actions

Malicious STP Case Symptoms

<table>
<thead>
<tr>
<th>CaseID: 26</th>
<th>Description</th>
<th>Related To</th>
<th>Details</th>
<th>Seen From</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>A procedure was recreated not by its original creator: move_to_platinum</td>
<td>Originally created by: GUARDIUM_QA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure was changed. A reference to a sensitive table was added to procedure: move_to_platinum</td>
<td>move_to_platinum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure was updated. The procedure contains a DDL command for an administrative/sensitive object: move_to_platinum</td>
<td>Table Name: user_groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure was updated. The procedure contains a DDL command for an administrative/sensitive object: move_to_platinum</td>
<td>move_to_platinum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Which web application was used as an entry point?
Which IP is the attack coming from?
Guardium GDPR Accelerator

3. GDPR Compliance

- Data Discovery and Classification for Personal Data
- Predefined Policies and Groups
- Auditing and Monitoring reports
- Support for GDPR Impact Assessment
- Workflows and Audit Process Builder for notifications to auditors, controllers and DPO
Security & Traceability – Infrastructure control and advanced threat detection

**EXTENSIVE DATA SOURCES**
- Security devices
- Servers & mainframes
- Network and virtual activity
- **Data activity**
  - Application activity
  - Configuration data
- Vulnerabilities and threats
- Users & identities
- Global threat intelligence

**IDENTIFICATION**
- Data collection, storage, and analysis
- Real-time correlation and threat intelligence
- Automatic asset, service and user discovery and profiling
- Activity baselining and anomaly detection

**REMEDIATION**
- Incident forensics
- Around-the-clock management, monitoring and detection
- Incident response

**QRadar Sense Analytics**

**Embedded Intelligence**
Guardium & QRadar integration
Optimizing security while expanding monitoring scope for data sources

- Improve analytics performance by offloading data analysis
- Save on storage costs for duplicating data audit logs
- Save on network bandwidth for data audit logs
- Real-time analysis and measures
- No need to turn audit logs on DB. Save on DB/App performance

Guardium

Real-time Activity

Normalized audit logs

QRadar Alerts and Data Discovery

Security Events and Audit Reports

File
Big Data
Data Warehouse
Database
Application
Network Infrastructure
Network Security
Servers
Mainframe
Identity
Incident Management – How we handle and respond to security incidents

IBM Resilient

PREVENTION
Help to stop attacks and remediate vulnerabilities

DETECTION
Identify threats with advanced analytics and forensics

RESPONSE
Respond to incidents in integrated and organized fashion

Unites Security Operations and Incident Response
Resilient will extend IBM’s offerings to create one of the industry’s most complete solutions to prevent, detect, and respond to threats

Delivers a Single Hub for Response Management
Resilient will allow security teams to orchestrate response processes, and resolve incidents faster and more effectively

Integrates with IBM and 3rd Party Solutions
Resilient integrates with QRadar and other IBM and 3rd party solutions so organizations of various sizes can successfully resolve incidents
Resilient Use Case: Breach Resolution

Inputs: System Intrusion information from external source

Resilient generates a GDPR/System Intrusion IR playbook:
- Disconnect compromised systems
- Analyse network traffic for signs of intrusion
- Notify Selected Supervisory Authority
- Post-incident review — update policies and procedures

Resilient INCIDENT RESPONSE PLATFORM

INCIDENT RESOLUTION

Mitigation: Block attack source

Threat Data/Asset information

IBM Security

Check Point

Malwarebytes

Microsoft Active Directory
Incident Response: the power of IBM Resilient

Every task has clear guidance instructions for the analyst.

The new breach notification timeline is already set and counting down when a simulation is started.

Tasks are split into phases of preparation.

Tasks can be assigned to team members with due dates for easy tracking.

Each task contains detailed instructions.
User Story: potential breach detected

- User activity is constantly monitored and tracked (Guardium):
  - Who did what ...
  - Data deletion, update, ..

- Suspicious activity detected (Guardium)

- Anomalous events also detected in network, OS application logs and in true traffic. An “offense” is created for the security analyst (QRadar)

- An incident is opened in Resilient to allow further investigation, tactic remediation actions, communication, notifications, long term remediation and security improvement (Resilient)
THANK YOU

FOLLOW US ON:
- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM’s current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.
Guardium Data Activity Monitor (DAM) for Data

Monitor and track data access and modification (databases and file systems)

- Continuous, policy-based, real-time monitoring of all data traffic activities, including actions by privileged users
- Behaviour analysis to detect outliers and spot anomalies
- Real-time alerting to prevent Data Loss
- Compliance automation; prepackaged compliance reports for SOX, PCI, GDPR, etc.
- Does not rely on resident logs that can easily be erased by attackers, rogue insiders (SOD enforcement for DBA access)
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- Minimal performance impact

Identify and respond to detected outliers with a convenient graphical interface

• Anomaly hours flagged red or yellow
• Click bubble for Outlier view