COBIT 5 and the GDPR

By Joanna Karczewska, CISA

COBIT Focus | 29 May 2017

With just a year left until the European Union’s (EU’s) General Data Protection Regulation (GDPR)\(^1\) takes effect, it is time for any organization with European customers to get started with the implementation of its requirements. Most supervisory authorities in EU countries have published guidelines on how to get ready. However, when it comes to information technologies involved, it would be convenient to find additional inspiration in a well-known governance of enterprise IT (GEIT) framework. And, yes, that framework is COBIT®.

It is useful to refer to an introductory document such as *The GDPR and You*,\(^2\) developed by the Office of the Data Protection Commissioner (DPC) of Ireland, to help organizations prepare for the GDPR. In order to provide clear guidance and a practical starting point, the DPC compiled a checklist to assist in moving toward 2018 and full compliance. By applying the COBIT® 5 enablers to the DPC road map, it is possible to determine the basic scope where COBIT can help.

**COBIT 5 Enabler: Processes**

As recommended by the DCP, the first step to take is to become aware of the upcoming legislative changes. The DCP states, “It is imperative that key personnel in your organisation are aware that the law is changing to the GDPR and start to factor this into their future planning. They should start to identify areas that could cause compliance problems under the GDPR.”\(^3\)

The relevant COBIT 5 process could be APO01 Manage the IT Management Framework and its management practices:

- **APO01.01 Define the organizational structure (figure 1):**
  - For establishing the involvement of stakeholders who will be critical to decision making concerning the GDPR implementation

  ![Figure 1—COBIT 5 Process APO01.01](image)

  Source: ISACA, *COBIT 5*, USA, 2012

- **APO01.02 Establish roles and responsibilities and its activities (figure 2):**
  - For establishing, agreeing on and communicating IT-related roles for all personnel in the enterprise who will be involved in the GDPR implementation with clearly delineated responsibilities and
accountabilities, especially for decision making and approvals. This will make all personnel involved aware of the new legislation and the need for compliance.

Figure 2—COBIT 5 Process APO01.02

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Description</th>
<th>Outputs</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO01.02 Establish roles and responsibilities. Establish, agree on and communicate roles and responsibilities of IT personnel, as well as other stakeholders with responsibilities for enterprise IT, that clearly reflect overall business needs and IT objectives and relevant personnel’s authority, responsibilities and accountability.</td>
<td>EDM01.01 Authority levels</td>
<td>Definition of IT-related roles and responsibilities</td>
<td>DSS05.04</td>
<td></td>
</tr>
<tr>
<td>EDM04.02 Assigned responsibilities for resource management</td>
<td>EDM04.02 Assigned responsibilities for resource management</td>
<td>DSS05.04</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP001.03</td>
<td>AP001.03</td>
<td>Definition of supervisory practices</td>
<td>EDM01.01</td>
<td></td>
</tr>
<tr>
<td>AP010.04</td>
<td>AP010.04</td>
<td>Quality management system (QMS) roles, responsibilities and decision rights</td>
<td>EDM01.01</td>
<td></td>
</tr>
<tr>
<td>AP003.01 Information security management system (ISMS) scope statement</td>
<td>AP003.01 Information security management system (ISMS) scope statement</td>
<td>EDM01.01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS06.03</td>
<td>DSS06.03</td>
<td>Allocated levels of authority</td>
<td>EDM01.01</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allocated roles and responsibilities</td>
<td>EDM01.01</td>
<td></td>
</tr>
</tbody>
</table>

Source: ISACA, COBIT 5, USA, 2012

The second step recommended by the DCP is to "make an inventory of all personal data you hold."4

The APO01.06 Define information (data) and system ownership management practice could apply (figure 3) for creating and maintaining an inventory of all personal data that will include information on the subject matter and duration of the processing, the nature and purpose of the processing, the type and special categories of personal data processed, where the data came from, who they are shared with, their retention periods, and the tools and techniques implemented to provide effective security of the personal data.

Figure 3—COBIT 5 Process APO01.06

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Description</th>
<th>Outputs</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO01.06 Define information (data) and system ownership. Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners make decisions about classifying information and systems and protecting them in line with this classification.</td>
<td>From</td>
<td>Description</td>
<td>Description</td>
<td>To</td>
</tr>
<tr>
<td>EDM01.01 Authority levels</td>
<td>From</td>
<td>Description</td>
<td>Data classification guidelines</td>
<td>AP003.02</td>
</tr>
<tr>
<td>EDM04.02 Assigned responsibilities for resource management</td>
<td>From</td>
<td>Description</td>
<td>Data security and control guidelines</td>
<td>BA02.01</td>
</tr>
<tr>
<td>AP001.03</td>
<td>From</td>
<td>Description</td>
<td>Data integrity procedures</td>
<td>BA02.01</td>
</tr>
<tr>
<td>AP010.04</td>
<td>From</td>
<td>Description</td>
<td>DSS05.04</td>
<td>DSS05.04</td>
</tr>
<tr>
<td>DSS06.03</td>
<td>From</td>
<td>Description</td>
<td>DSS06.01</td>
<td>DSS06.01</td>
</tr>
</tbody>
</table>

Source: ISACA, COBIT 5, USA, 2012

Another key issue is the implementation of the new rights and the strengthening of current rights of individuals under the GDPR. The information that organizations are obliged to supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge

Therefore, as recommended by DCP, organizations should review and update procedures for handling requests from data subjects within the new timescales. But the COBIT 5 process that directly addresses communication to stakeholders—in this case data subjects—is EDM05 Ensure Stakeholder Transparency and its key governance practices:

- EDM05.01 Evaluate stakeholder reporting requirements, including data privacy notices
The responsible, accountable, consulted and informed (RACI) chart for this process (figure 4) may need to be extended to include:

- Officers who will handle requests from individuals
- Public relations officers who will be issuing official statements and handling media communications if a personal data breach is made public

The GDPR also requires the controller to notify the supervisory authority about the personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. The basic challenge for controllers will be to record, classify and prioritize requests and incidents, so as to identify personal data breaches as soon as possible and determine whether the breach is likely or not to result in a risk to the rights and freedoms of natural persons. The relevant COBIT 5 process is DSS02 Manage Service Requests and Incidents. Additionally, new procedures that have to be set in place concern:

- The notification of a personal data breach to the supervisory authority
- The communication of a personal data breach to the data subject

In the next few months the Article 29 Working Party intends to produce a guidance document on the notification of personal data breaches. This guidance will help manage the DSS02 process in compliance with the new regulation.

Last, but not least, the GDPR also requires controllers to carry out data protection impact assessments (DPIAs) where processing operations are likely to result in a high risk to the rights and freedoms of natural persons and to ensure data protection by design and by default. This implies high maturity levels of 2 COBIT 5 processes:

- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build

Efforts should be concentrated on the management practice BAI02.03 Manage requirements risk, which requires identifying, documenting, prioritizing and mitigating functional, technical and information processing-related risk associated with the enterprise requirements and proposed solutions—in this case, the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

The Article 29 Working Party has recently published Guidelines on DPIA, determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. This document includes a list of existing EU DPIA frameworks. One of the most useful is a set of documents on privacy impact assessment (PIA) published by the French Commission Nationale de l’Informatique et des Libertés (CNIL).

---

8, 9, 10
COBIT 5 Enabler: Information

The GDPR sets principles relating to processing of personal data. One of them states that personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Another requires personal data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

In terms of information quality goals as defined in COBIT® 5: Enabling Information, personal data have to be:

- **Accurate**—Data are correct and reliable.
- **Objective**—Data are unbiased, unprejudiced and impartial, especially in case of automated individual decision making, including profiling.
- **Complete**—Data are not missing and are of sufficient depth and breadth for the task at hand.
- **Current**—Data are sufficiently up to date for the task at hand.
- **Secure/accessible/available**—Data are available when required, or are easily and quickly retrievable.
- **Secure/accessible/restricted access**—Data are restricted appropriately to authorized parties.

COBIT 5 Enabler: Culture, Ethics and Behavior

As mentioned previously, awareness is a key factor for the effectiveness of the GDPR. So, the COBIT 5 enabler Culture, Ethics and Behavior, which refers to the set of individual and collective behaviors within an enterprise, becomes of key importance.

The good practices for creating, encouraging and maintaining the desired behavior throughout the enterprise concerning the protection of personal data—as listed in the COBIT 5 framework—should include:

- Communication throughout the enterprise of desired behaviors
- Awareness of desired behavior, strengthened by the example behavior exercised by senior management and other champions, including the data protection officer
- Incentives to encourage and deterrents to enforce desired behaviour
- Rules and norms, which provide more guidance on desired organisational behaviour

COBIT 5 Enabler: Principles, Policies and Frameworks

The GDPR requires the controller to implement appropriate data protection policies.

When developing new procedures concerning the processing of personal data or reviewing current ones, good policies—as recommended in the COBIT 5 framework—should be:

- **Effective**—They should achieve the stated purpose.
- **Efficient**—They should ensure that the GDPR principles are implemented in the most efficient way.
- **Nonintrusive**—They should appear logical for those who have to comply with them, i.e., they do not create unnecessary resistance.

Also, there should be a mechanism to provide easy access to these policies for all stakeholders and stakeholders should know where to find these policies.

Security

Only article 32 of the GDPR refers explicitly to the security of processing that controllers and processors have to ensure by implementing appropriate technical and organizational measures taking into account the state of the art; the costs of implementation; and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. These measures should include:
• The pseudonymization and encryption of personal data
• The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
• The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
• A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

However, more security requirements are mentioned in other articles of the GDPR. Having an information security management system would definitely prove an advantage. This implies a well-managed APO13 Manage Security process.

Conclusion

This mapping of COBIT 5 enablers to the GDPR is not exhaustive, and readers should apply their own professional judgment to ensure that their preparations take account of all actions required to bring their organizations into compliance with the new law. The intention here is to show that COBIT 5 can prove very useful in supporting these actions and to inspire COBIT 5 users.

Joanna Karczewska, CISA

Is an independent IS auditor, COBIT consultant and trainer, lecturer at the Warsaw Technical University (Poland) and the Polish Naval Academy, author of numerous articles on COBIT and IT audit, and speaker at IT conferences. She has 40 years of IT professional experience working for Polish government agencies and foreign companies based in Poland. Karczewska served as an expert reviewer of many COBIT 5 publications. She is also the community leader of the Poland topic of ISACA's Knowledge Center.

Endnotes

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), effective 25 May 2018
2 Office of the Data Protection Commissioner, The GDPR and You, Ireland, 2017
3 Ibid.
4 Ibid.
5 European Commission, Article 29 Working Party, 22 November 2016
6 Ibid.
7 Commission Nationale de l’Informatique et des Libertés, Gérer les risques, 2 March 2017
8 Commission Nationale de l’Informatique et des Libertés, Privacy Impact Assessment (PIA) Methodology (How to Carry Out a PIA), June 2015
10 Commission Nationale de l’Informatique et des Libertés, Measure for the Privacy Risk Treatment Good Practices, France 2012