Deloitte.

Data Protection Control Framework

GDPR

How do you monitor your ongoing compliance with the General Data Protection Regulation (GDPR)?

How can you ensure data protection risks and regulatory requirements are continuously considered and addressed?

See how you can operationalize your data protection controls and track their operating effectiveness over time.

Your Challenge

Your organization has made significant efforts to achieve compliance with the GDPR. **Data Protection measures** (e.g., record of processing activities, data processing agreements, etc.) involving various stakeholders in the organization (e.g., Business functions, IT, Legal, HR, etc.) have been designed and implemented. Now you have to ensure that these measures operate effectively in order to maintain your compliance while continuously adjusting to the ever-changing regulatory requirements, and to data protection risks arising from new business opportunities. Are you adequately prepared for that?

Below a few questions to see where you stand:

- Have you defined a process to regularly assess the operating effectiveness of your data protection measures and take remedial actions when required?
- Have you clearly defined the roles, responsibilities and reporting channels to support execution and follow-up of these measures?
- Have you defined key risk and performance indicators to measure and report on the effectiveness of the data protection measures to the management of your organization?

Have a look at our proposed **Data Protection Control Framework** solution to point you in the right direction.

Our solution

The Data Protection Control Framework is a comprehensive solution aiming at helping to **establish, assess and enhance your data protection measures** to ensure ongoing compliance with the GDPR. Our proposed solution leverages the proven COSO Internal Control Framework[1], while also considering the certification criteria of the CNPD's GDPR-Certified Assurance Report Based Processing Activities (GDPR-CARPA)[2].

Our **solution can be tailored to your organization** considering your objectives, needs, risk appetite, size or industry.

Data Protection Control Framework components

The Data Protection Control Framework consists of **5 key components** deployed through a combination of **Governance**, **Processes** and **Technology** for the various levels (e.g., entity, department, unit, etc.) of the organization.

Control Environment – focuses largely on the attitude, level of awareness and actions of those in charge of the organization's governance (i.e., tone at the top).

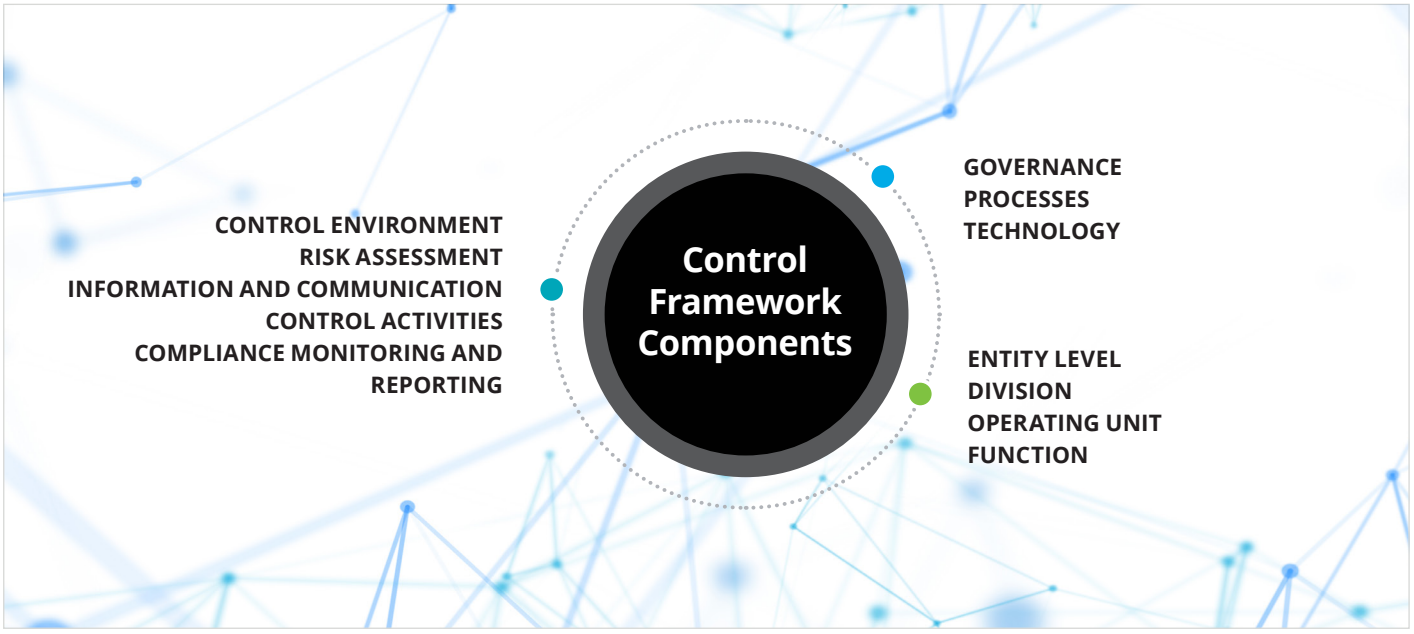
Risk Assessment – forms the basis for how the organization identifies and manages the data protection risks associated with processing activities documented in the record (Article 30 of the GDPR).

Information and Communication – defines the channels in place to address data protection matters, internally within the organization and externally with data subjects, authorities and business partners.

Control Activities – summarizes all legal, organizational and technical measures to ensure that personal data is processed and protected in an adequate manner in compliance with GDPR requirements (and other applicable data protection regulatory requirements).

Compliance Monitoring and Reporting – forms the processes to assess the design, implementation and operating effectiveness of the measures deployed within the organization and to report on their performance and potential risks.

1. COSO Internal Control Framework: https://www.coso.org/Pages/ic.aspx
2. GDPR-CARPA certification criteria: https://cnpd.public.lu/fr/actualites/national/2019/07/Certification.html



How Deloitte can help

01

You will meet with our specialists to first understand your environment and **define the scope of your Data Protection Control Framework** that aligns with your organization's objectives and needs.

02

We will assist you in **designing** of the various **components of the Framework** by building upon what you have already put in place, e.g., data protection policy, governance model, risk assessment process, data protection measures, etc.

03

We will help you define the **process and monitoring** activities aiming at assessing your data protection measures on a regular basis. This will include designing a detailed monitoring plan. We will also assist you with building a comprehensive set of **key risk and performance indicators** to help you evaluate and improve the efficiency of each component of your Framework.

04

We will help you with the **deployment of the Framework** by determining the deployment strategy and priorities, providing trainings to the relevant stakeholders and supporting you with the implementation of the monitoring activities. This will include designing testing plans and procedures for each activity.

Our GDPR expertise combined with our hands-on experience in deployment of internal control frameworks, supported by our library of "ready-for-use" templates, will help accelerate the process of setting up and deploying the Data Protection Control Framework for your organization.

Contacts

Roland Bastin
Partner - Governance, Risk & Compliance
+352 451 452 213
rbastin@deloitte.lu

Laurent Berliner
Partner - Governance, Risk & Compliance
+352 451 452 328
lberliner@deloitte.lu

Irina Hedea
Partner - Governance, Risk & Compliance
+352 451 452 944
ighedea@deloitte.lu

Georges Wantz
Managing Director - Technology & Enterprise Application
+352 451 454 363
gwantz@deloitte.lu

Deloitte.

Deloitte Luxembourg
20 Boulevard de Kockelscheuer
L-1821 Luxembourg
Grand Duchy of Luxembourg

Tel.: +352 451 451
www.deloitte.lu