Corporate Compliance & Conduct, Boadilla del Monte, December 2020

Data Protection Corporate Governance Model

Sencillo | Personal | Justo
Simple | Personal | Fair

Santander

Content

1. **Framework.**

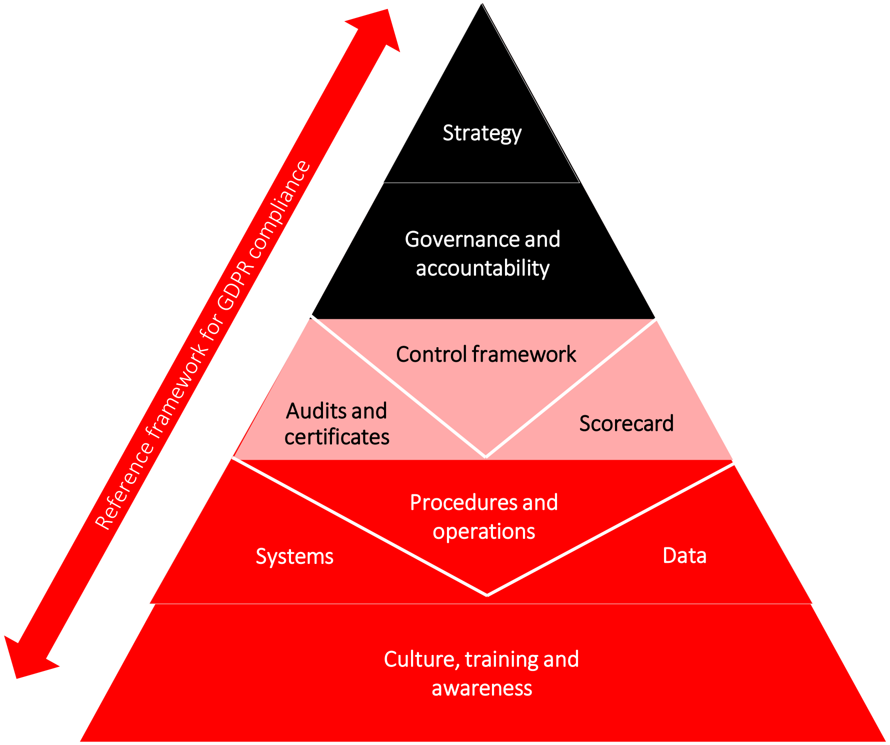
2. Data protection heads.
   - Organisational structure of the model.

3. Functions and responsibilities.

1.- Framework.

Layered structure of the reference framework

To successfully address the proper management of the compliance with data protection regulations a number of components operate in a coordinated manner and in line with the defined strategy and the following framework that defines its key elements.


Reference framework for GDPR compliance
Strategy
Governance and accountability
Control framework
Audits and certificates
Scorecard
Procedures and operations
Systems
Data
Culture, training and awareness

Governance layer:

- *Governance* structure which organises and appropriately establishes the roles and responsibilities.
- Policies and general framework to all components of the reference framework.

Monitoring and control layer:

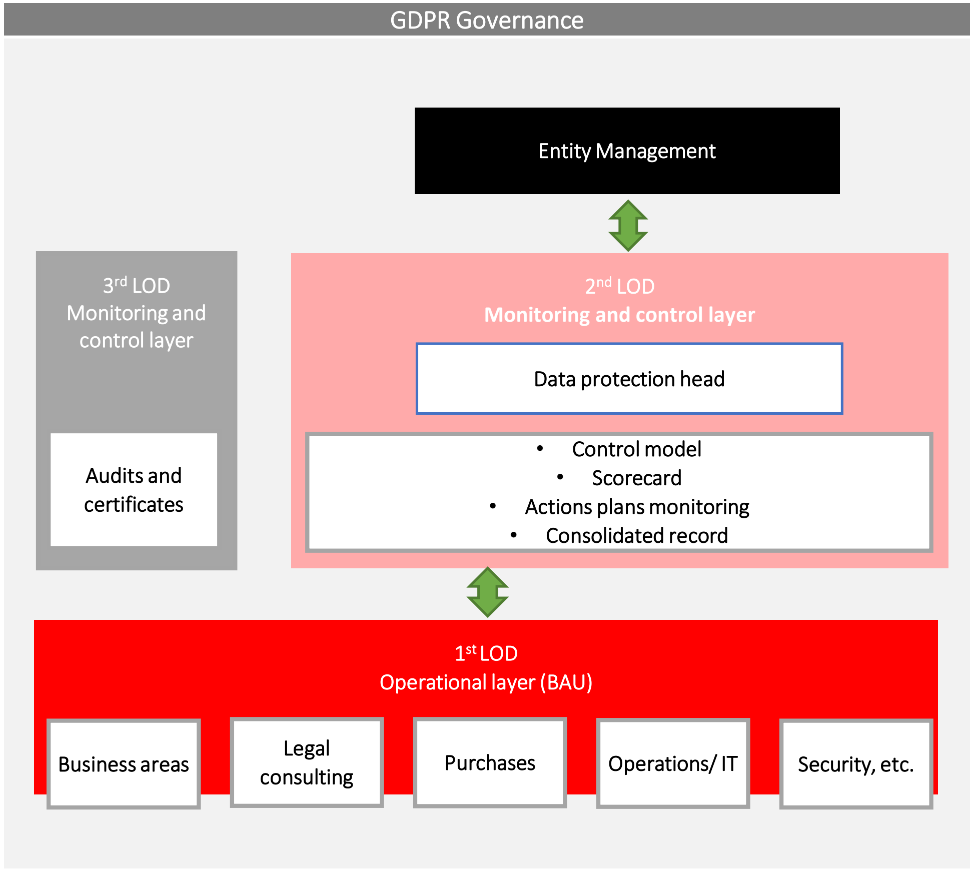
- Control model based on 3 LoD.
- Scorecard that enable the decision making.
- Following up of the mitigating actions plans

Operational layer:
Set of processes, procedures and operations that provide operational support to GDPR compliance. They must be properly coordinated with the monitoring and control layer, in accordance with the governance layer.

1.- Framework.

Lines Of Defence (LOD)

The data protection governance model at a entity level fits into the corporate/group governance model.



3rd LOD:

Independent view on the organization compliance degree of the privacy management, taking as a reference the current regulation, as well as existing policies and procedures.

2nd LOD:

Monitoring of privacy activities management to be carried out by the 1st LOD. This 2nd LOD must ensure that privacy risks are managed in accordance with the risk appetite formulated by the entity management and will promote a solid culture of risk an compliance across the organization.

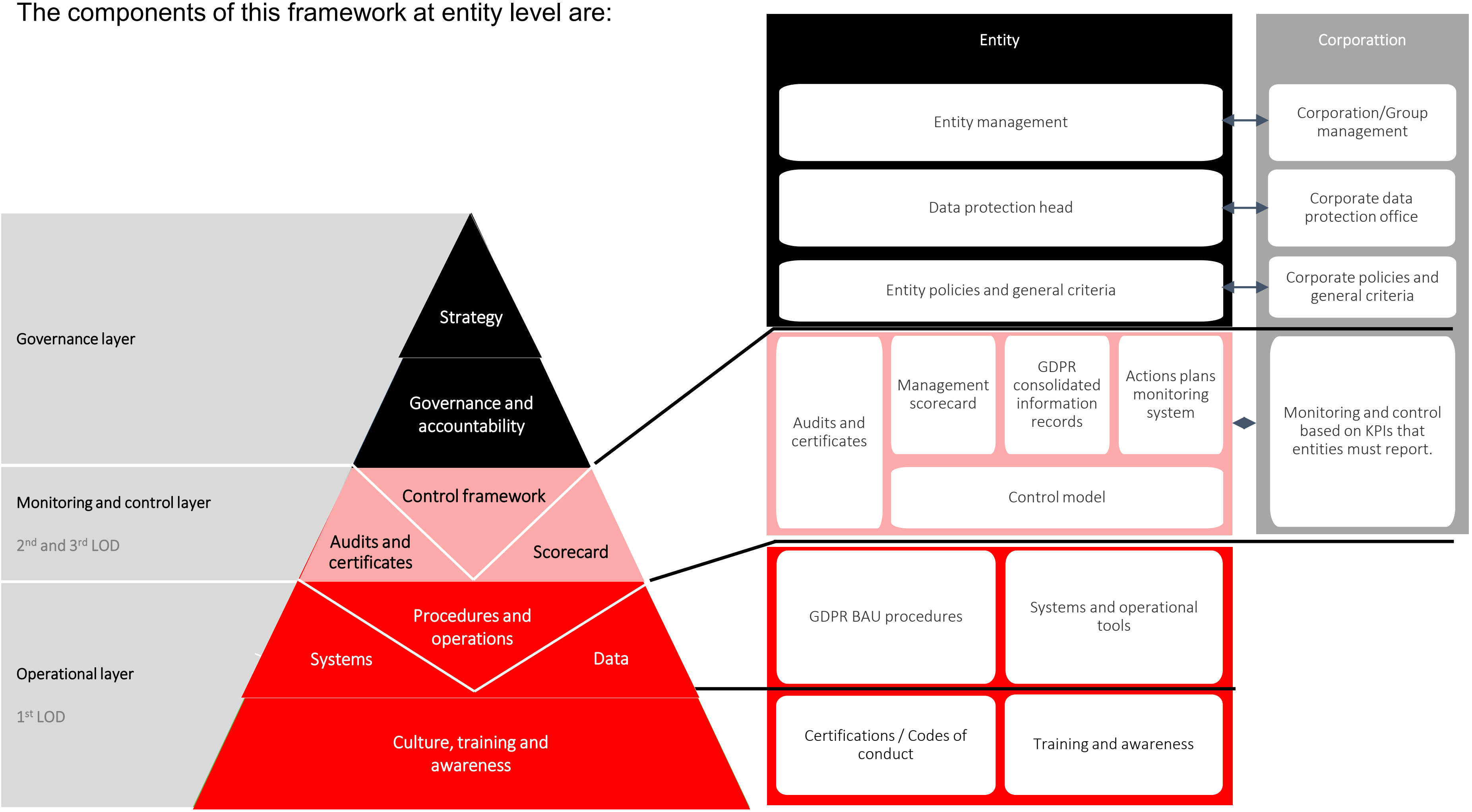
1st LOD:

Business and support units, as responsibles for the execution of the business as usual (BAU) activities according to the defined policies and procedures. They must be properly trained and aware about privacy matters and existing policies and procedures, and proviced with sufficient resources to do so effectively.

1.- Framework.

Lines Of Defence (LOD)

The components of this framework at entity level are:



Governance layer

Monitoring and control layer

2nd and 3rd LOD

Operational layer

1st LOD

Strategy

Governance and accountability

Control framework

Audits and certificates

Scorecard

Procedures and operations

Systems

Data

Culture, training and awareness

Entity

Entity management

Data protection head

Entity policies and general criteria

Audits and certificates

Management scorecard

GDPR consolidated information records

Actions plans monitoring system

Control model

GDPR BAU procedures

Systems and operational tools

Certifications / Codes of conduct

Training and awareness

Corporattion

Corporation/Group management

Corporate data protection office

Corporate policies and general criteria

Monitoring and control based on KPIs that entities must report.

Content

1. Framework.
2. **Data protection heads.**
    - Organisational structure of the model.
3. Functions and responsibilities.

2.- Data protection heads.

Three main figures display the highest level of responsibility in terms of compliance with data protection provisions:

Local

DPO/Head

Data protection **maximum** authority

1. Point of contact with the Supervisory Authority and data subjects
2. Cooperation with the **Supervisory** Authority
3. Data protection advice
4. Control and monitoring
5. Training
6. DPIAs advise
7. Realization of the prior consultations to the **Supervisory** Authority
8. Monitoring of processing activities record
9. Assess on security breach communication
10. Assess on third parties management
11. Monitoring of data subjects rights exercise

Champion

SME in the unit or entity

1. Internal point of contact **as first level of support.**
2. **Channel for resolving and/or addressing questions and support requests**:
   a) To the corporate data protection office, in the case of units and corporate entities.
   b) To the DPO/Head/Heads **of the jurisdiction, in the case of other** entities.
3. Responsible for the internal distribution of criteria, procedures, and other instructions

Corporate

Corporate data protection office

GDPR compliance global supervisor

1. Monitoring the data protection compliance of the Group
2. Consolidated reporting to the senior management of the Group
3. Point of communication with the competent authorities at a global level
4. Impact assessment of security incidents at **a** global level
5. Data protection global risks assessment
6. Facilitate corporate criteria and be the point of contact at a corporate level for the entity's DPOs

Support the DPO/Head and champions of the units and corporate entities

1. Provide expert advice on the regulation and support the DPOs/Heads and champions on the execution of their functions

2.- Data protection heads.

Each entity or unit subject to data protection provisions has appointed a head of data protection, which may be a DPO/Head or a "champion" on the basis of the following criteria.

1. **Group subsidiaries.**

For those subject to GDPR requirements, a DPO is formally appointed should any of the following assumptions are met:

Assumption
Regular and systematic observation of data subjects on a large scale.
Personal data special categories (e.g. ethnic or racial origin, political opinions, trade union membership, health data, convictions and offence penalties, etc.)
In cases where required by law of the Union or the Member States. For example, according to the Spanish law and local competent supervisory authority, it will be necessary to appoint a DPO for credit institutions and entities that provide investment services.

Group entities that meet at least one of the assumptions have a **<u>DPO</u>** which responds directly to the local competent supervisory authority and the data subjects. Otherwise, a **<u>data protection</u>** ***<u>champion</u>*** has been appointed.

Likewise, on those jurisdictions outside the EEA, data protection heads have been appointed.

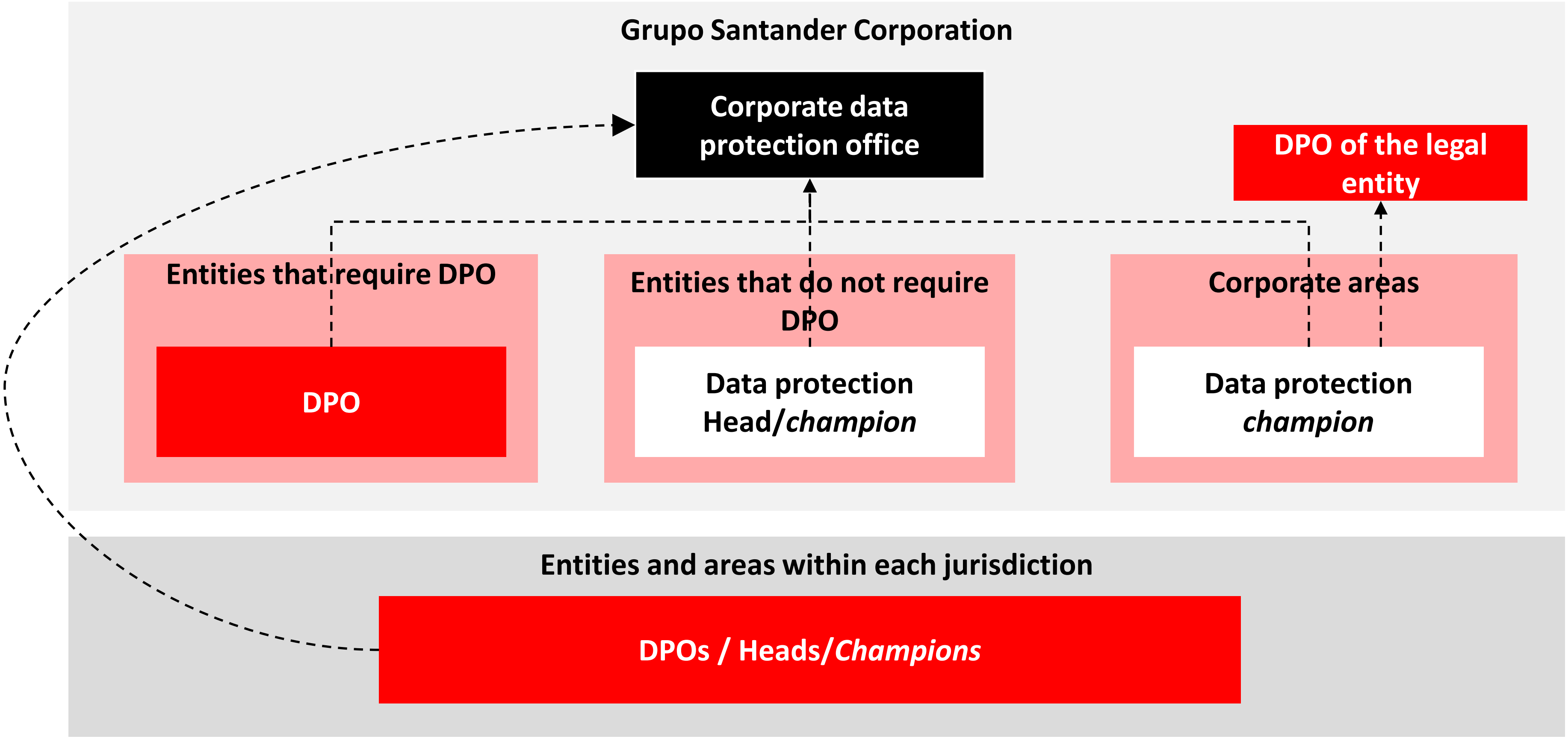
2. **Units and corporate areas.**

Units that process personal data have appointed a champion figure that supports the DPO/Head of the entity to which they belong.

2.- Data protection heads.

c. Organisational structure of the model

The governance model has the following organizational structure and relationship model among the data protection responsible figures:


Grupo Santander Corporation
Corporate data protection office
DPO of the legal entity
Entities that require DPO
DPO
Entities that do not require DPO
Data protection Head/*champion*
Corporate areas
Data protection *champion*
Entities and areas within each jurisdiction
DPOs / Heads/*Champions*

Content

1. Framework

2. Data protection heads

   - Organisational structure of the model

3. **Functions and responsibilities**

3.- Functions and responsibilities

- **R - Responsible**: Responsible for the execution of task.
- **A - Accountable**: Responsibility for that task to be executed.
- **C - Consulted**: Figure that must be consulted to perform the task.
- **I - Informed**: Figure that must be informed of the implementation of the task.

Components / Roles		Corporate / Group management	Corporate data protection office	Entity management	DPO/Head	Champion, in case one exists	Area responsible for processing activity	Processing activity processor	Other areas
Governance model	Governance model definition	I	I	C, I	R, A	C, I	I	I	I
Representation and institutional aspects	Point of contact with the supervisory authority and the data subjects	I*	I	I*	R, A	C	C		
	Cooperation with the supervisory authority	I*	I	I*	R, A	C	C		
Operational aspects	Local policy definition	I*	C, I	A, C	R	C, I	I	I	I
	Regulatory changes identification and setting up criteria	I*	C, I	C	R, A	C, I	I	I	I
	Provide advice on data protection		C		R, A	R**	C, I	I	I
	BAU procedures adaptation	I*	I	I*	A, C	C	I	C	R
	Identification and evaluation of possible new processing activities				A, C	A,C**	R	C	
	Risk methodology definition (includes risk appetite)	I*	I	I*	A, R	I	I		C (p.e. Risks)
	Risk assessment pre-DPIA and DPIAs production		I	I*	A, C	A,C**	R	C	C (p.e. CISO, Risks, Legal)
	Prior consultation to the supervisory authority		I	C, I	A, R	C	C, I		
	Updated maintenance of the processing activities record		I	I*	A, I	C, I	R	C	C (p.e. CISO, Legal, etc.)

* At discretion of the DPO/Corporate Data Protection Office

** Responsibility in the first instance, shared with the DPO in case it cannot be assumed

*** Units without DPO

3.- Functions and responsibilities

- **R - Responsible**: Responsible for the execution of task.
- **A - Accountable**: Responsibility for that task to be executed.
- **C - Consulted**: Figure that must be consulted to perform the task.
- **I - Informed**: Figure that must be informed of the implementation of the task.

Components / Roles		Corporate / Group management	Corporate data protection office	Entity management	DPO/Head	Champion, in case one exists	Area responsible for processing activity	Processing activity processor	Other areas
Operational aspects	Obtaining consents and compliance with reporting obligations				**A**	**I**	R	R	R (p.e. business, operations)
	Security incidents identification				A	I	R	R	R (p.e. CISO)
	Security incidents evaluation and communication	I	I	I	R, A	**R***,A,**C	C	C	C (p.e. CISO, business, etc.)
	Third parties homologation		**I, C**	I*	**A, I**	I	C	C	R (p.e. procurement, Service manager, etc.)
	Third parties contracts management			I*	A, I	I	C	C	R (p.e. Aquanima, Legal)
	Third parties compliance monitoring			I*	A, I	I	C	C	R (p.e. Aquanima, procurement)
	Attention to requests for exercise of rights of data subjects		I	I*	A	A	C	C*	R (p.e. operations, Legal)
	Operational and IT changes implementation (according to procedures and DPIAs)			I*	A, C	C**	R	I	R (p.e. IT)
	BAU operations execution according to procedures and criteria			I*	A	A	R	I	R
	Execution of training and awareness actions			I*	A	A	C		R (p.e. Training)

* At discretion of the DPO/Corporate Data Protection Office

** Responsibility in the first instance, shared with the DPO in case it cannot be assumed

*** Units without DPO

3.- Functions and responsibilities

- **R - Responsible**: Responsible for the execution of task.
- **A - Accountable**: Responsibility for that task to be executed.
- **C - Consulted**: Figure that must be consulted to perform the task.
- **I - Informed**: Figure that must be informed of the implementation of the task.

Components / Roles		Corporate / Group management	Corporate data protection office	Entity management	DPO/Head	Champion, in case one exists	Area responsible for processing activity	Processing activity processor	Other areas
Internal Control Model for each Entity/Area	Control model definition		I	I	A, C	A,C**	C	C	R (Compliance and 1st LOD areas)
	Controls execution				A, I	A,I	I		R (controls responsibles)
	Compliance monitoring	I*	I	I*	A, R	A,C, I	I	C	C **(controls responsibles)**
Scorecard (Corporation-subsidiary relationship model)	Definition of scorecard management system		A, R		C, I	C, I			
	Indicators reporting		I	I*	A, R	R**			
	Indicators analysis	I*	A, R		A,C, I	A,C, I			
Relevant aspects and critical incident management	Relevant aspects and critical incidents **management**	I*	C, I	C, I	A, R	A,C	C	C	C

* At discretion of the DPO/Corporate Data Protection Office

** Responsibility in the first instance, shared with the DPO in case it cannot be assumed

*** Units without DPO

Our purpose is to help people and businesses prosper.

Our culture is based on the belief that everything we do should be

Simple | Personal | Fair

Santander