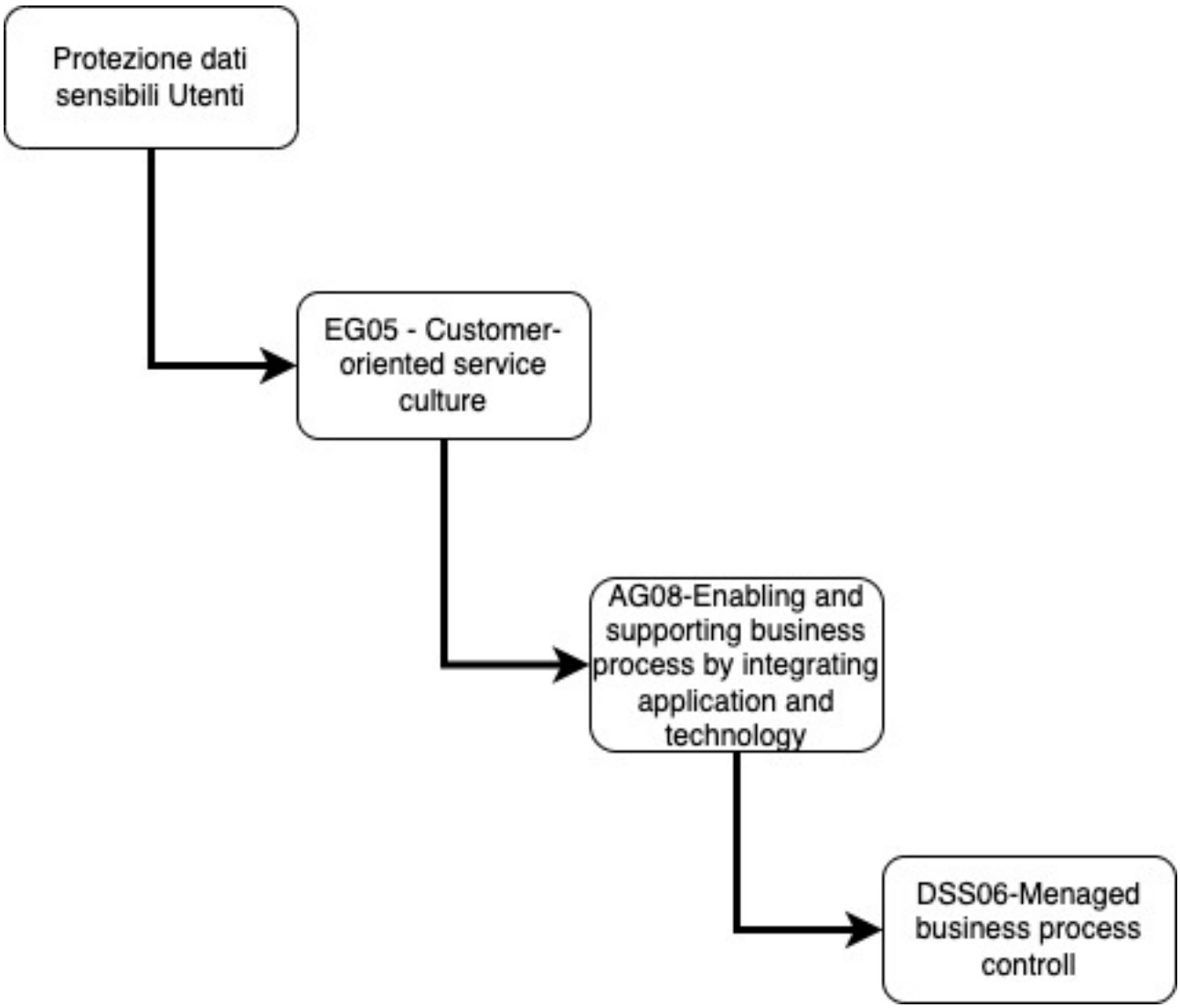
CONSEGNA 13 MAGGIO S3L2

L'Alta Direzione ha stabilito di aver bisogno che i dati sensibili degli utenti siano protetti, in conformità alle normative per migliorare anche la fiducia del cliente verso l'organizzazione (l'esigenza non si riferisce alla business continuity, non è richiesto Design Factors e Focus Area).

- collega a questo bisogno, un Enterprise Goal tra quelli in «A-Figure 4.17»
- collega all'EG scelto, un Alignment Goal tra quelli in «A-Figure 4.18», può essere di aiuto la «B-Figure A.1»
- collega all'AG scelto, un Governance and Management Objectives, tra quelli in «B-Chapter 4», può essere di aiuto la «B-Figure A.2»
- scegli una pratica che possa concorrere a soddisfare l'esigenza dell'Alta Direzione tra le pratiche presenti all'interno dell'elemento scelto precedentemente. B/D
- Quali sono i ruoli e le responsabilità per questa pratica? B/C
- Quali sono gli input/output per questa pratica? B
- In quale documento aziendale dovrebbe essere descritta la policy o la procedura? B

COBIT GOAL CASCADE



EG06	Customer	Business service continuity and availability	• Number of customer service or business process interruptions causing significant incidents • Business cost of incidents • Number of business processing hours lost due to unplanned service interruptions • Percent of complaints as a function of committed service-availability targets

AG08	Internal	Enabling and supporting business processes by integrating applications and technology	• Time to execute business services or processes • Number of I&T-enabled business programs delayed or incurring additional cost due to technology integration issues • Number of business process changes that need to be delayed or reworked because of technology integration issues • Number of applications or critical infrastructures operating in silos and not integrated

Management	Deliver, Service and Support	DSS06	Managed Business Process Controls	Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements. Manage and operate adequate input, throughput and output controls (application controls) to ensure that information and information processing satisfy these requirements.	Maintain information integrity and the security of information assets handled within business processes in the enterprise or its outsourced operation.

B. Component: Organizational Structures

Key Management Practice	Executive Committee	Chief Information Officer	I&T Governance Board	Chief Information Security Officer	Business Process Owners	Data Management Function	Service Manager	Information Security Manager	Legal Counsel
DSS06.01 Align control activities embedded in business processes with enterprise objectives.	R		A		R				
DSS06.02 Control the processing of information.		R	A	R	R	R			R
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.		R	A	R	R			R	
DSS06.04 Manage errors and exceptions.		R		R	A		R		
DSS06.05 Ensure traceability and accountability for information events.		R		R	A				
DSS06.06 Secure information assets.		R		R	A				

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this component	

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority. Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	a. Number of incidents and audit findings due to access or separation-of-duties violations b. Percent of business process roles with assigned access rights and levels of authority c. Percent of business process roles with clear separation of duties

Activities	Capability Level
1. Allocate roles and responsibilities based on approved job descriptions and business process activities.	2
2. Allocate levels of authority for approval of transactions, transaction limits and any other decisions relating to the business process, based on approved job roles.	
3. Allocate roles for sensitive activities so there is a clear segregation of duties.	
4. Allocate access rights and privileges based on the minimum that is required to perform job activities, based on pre-defined job roles. Remove or revise access rights immediately if the job role changes or a staff member leaves the business process area. Periodically review to ensure that the access is appropriate for the current threats, risk, technology and business need.	3
5. On a regular basis, provide awareness and training regarding roles and responsibilities so that everyone understands their responsibilities; the importance of controls; and the security, integrity, confidentiality and privacy of company information in all its forms.	
6. Ensure administrative privileges are sufficiently and effectively secured, tracked and controlled to prevent misuse.	
7. Periodically review access control definitions, logs and exception reports. Ensure that all access privileges are valid and aligned with current staff members and their allocated roles.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
HITRUST CSF version 9, September 2017	13.04 Collection, Use and Disclosure
ISO/IEC 27002:2013/Cor.2:2015(E)	7. Human resource security
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 5: Controlled Use of Administrative Privileges

Management Practice	Example Metrics
DSS06.04 Manage errors and exceptions. Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	a. Frequency of processing inefficiencies due to incomplete data entry b. Number of errors detected in a timely manner c. Number of data processing errors that were efficiently remediated

Activities	Capability Level
1. Review errors, exceptions and deviations.	2
2. Follow up, correct, approve and resubmit source documents and transactions.	
3. Maintain evidence of remedial actions.	
4. Define and maintain procedures to assign ownership for errors and exceptions, correct errors, override errors and handle out-of-balance conditions.	3
5. Report relevant business information process errors in a timely manner to perform root cause and trending analysis.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.	APO11.01	Quality management system (QMS) roles, responsibilities and decision rights	Allocated levels of authority	APO01.05
	APO13.01	Information security management system (ISMS) scope statement	Allocated roles and responsibilities	APO01.05
	DSS05.05	Access logs	Allocated access rights	APO07.04
	EDM04.02	Assigned responsibilities for resource management		

E. Component: Principles, Policies and Procedures			
Relevant Policy	**Policy Description**	**Related Guidance**	**Detailed Reference**
Business controls guidance	Defines business process controls to ensure proper control and reduce risk of fraud and errors. Identifies manual controls to protect documents (e.g., source, input, processing and output documents); identifies supervisory controls to review the flow of documents and ensure correct processing. Includes I&T general controls (e.g., physical security, access and authentication, and change management) and application controls (e.g., edit checking, system configuration and security settings).		

G. Component: Services, Infrastructure and Applications
• Automated application controls • Event log auditing tools