Standard Operation Procedures	SOP_048_Govern Technology and Transformation
27/11/2023	**Public**

Govern Technology and Transformation

Special Requirements	This procedure is a controlled document maintained by Quality Management. It may not be deleted without comparable controls. Please note that this document becomes uncontrolled once printed. Make sure by always referring only to the Repository that you have the right version in use. Deviations from the provision of this document need to be recorded in the Exception Request Workflow. The procedure should be updated when there are changes in EFSA with respect to what is stated in the document (e.g. Relevant Standards, legislation, and documents, change in procedure, etc.). The person responsible for maintaining this procedure up to date is the Lead author with the support of the QM.

Process Responsibility	Process owners are accountable this procedure being adhered to within their respective or unit. All relevant staff is responsible for the correct implementation of the procedure. Responsibilities for performing specific steps are outlined in the document.

SCOPE AND OBJECTIVES

IT Technology and software systems are fundamental enablers to the EFSA's strategy, business processes and data analysis. How technology is selected, implemented and managed has an impact on whether the organisation achieves its vision, mission and objectives.
IT Governance is mandatory for an organisation like EFSA. Here are the core strategic aspects in scope:

- **Value creation**: Any new project or change must be carefully assessed and must follow pre-defined specific processes, including cost-benefit analysis
- **Risk management**: EFSA's core processes are dependent on IT – the security and EUDPR compliance, the performance and the continuity of the business processes.
- **Continuous improvement**: EFSA must stay abreast of technological innovation in terms of new products, innovative services and revised processes so that opportunities to improve KPIs are readily seized.

The EFSA IT Governance is applied at two different levels:

- At strategic level
- At operational (or project and processes) level

The main objectives addressed and guaranteed at each level are (S=Strategic level, O=Operational level):

- To have complete alignment between IT and strategic business goals (S, O).
- To establish organisation, IT application, technology infrastructure and services to support the EFSA business strategy (S, O).
- To monitor the achievement of the goals and the performance level of the IT services supporting the business processes (S, O).
- To maximise the skill and competence of the people involved in IT (S, O).

- To manage the IT process according to the best practices on the market (O).
- To establish policies, and procedures (O).

The present SOP_048 Govern Technology and Transformation and SOPs 047 Advice, 052 Transform, 049 Deliver Services, 050 Enhance products and services, 053 Scan, 058 Innovate, 054 Semi Agile describe processes, best practices, and rules to be applied at the strategic and operational level.

EFSA Process Architecture

In the framework of the EPA 3 process Architecture, this SOP is part of these processes: 12.1 "Strategy, Planning, Analysis", 13.1 "Enterprise Architecture", 5.6 "Digital Services", and 12.3 "Quality Management".

RELEVANT STANDARDS, LEGISLATION AND DOCUMENTS

The following international standards apply for this process

- COBIT
- ISO/IEC 38500
- ITIL 4
- TOGAF 9
- DAMA
- BABOK 3.0
- ISO 9001 Quality Management System
- PM² project management methodology
- Methodology for carrying out a Data Protection Impact Assessment (DPIA) prior to introducing new technologies when and if critical to personal data processing

ABBREVIATIONS AND DEFINITION

A&S	Architecture & Solutions Team (within TS)
CORSER	Corporate Services Unit
DPO	Data Protection Officer
DW	Digital Workplace Team (within CORSER)
EA	Enterprise Architecture
EDM	Evaluate Direct Monitor
EUDPR	Data Protection Regulation (EU) 2018/1725
KNOW	Knowledge, Innovation and Partnership Management Unit
ISO	Information Security Officer
MT	Management Team
POTI	Process, Organization, Technology, Information. A common business model for transformation adopted by EFSA.
RfC	Ready for Closing

RfE	Ready for Execution
RfP	Ready for Planning
TP	Transformation Partners Team (within TS)
TPMO	Transformation PMO Team (within TS)
TS	Transformation Services Unit
PROCEDURE	
	This is the overarching TS SOP. Previous SOPs in the process: SOP_051 Corporate Planning and Monitoring
Step 1	**1.0 Define the IT Plan as a function of EFSA strategy**
Management Team Chair - Executive Director Participate - Heads of Department - Chair of Preparedness Council - Others on demand TS	In parallel with the EFSA strategy definition by the Management team (see SOP on Corporate planning and monitoring), TS is responsible for drafting the IT strategic principles, IT strategic capabilities, and mapping of business capabilities to technology platforms and solutions, visualisation of the as-is and target enterprise architecture, as well as in updating the IT methodologies that support EFSA in the achievement of the strategic objectives, according to the EFSA Decision Making Framework and Accountability Framework. These, together, can be called the **IT Plan** The IT Plan and methods must specify: • the missions, the performance ambition, and the top-level KPIs • the high-level IT transformation plan • the IT financial investment to support the new strategy • the organisation, resources, competence, and skills • the cost/benefit and risks correlated For designing the IT Plan, TS will follow the best practices as described in COBIT 5, and TOGAF 9, and use the tools and methods of BABOK 3.0.
Step 2	**2.0 Define and review the IT Plan**
- Preparedness Council (Accountable) - TS HoU (Responsible) - A&S (Responsible) - TP (Responsible) - DW (Consulted) - ISO/DPO (Consulted)	**Update the target Enterprise Architecture and IT Plan** Whenever a new IT Plan is defined, **A&S and TP must prepare the revised enterprise architecture to-be state** and identify financial and organisational impacts following these IT principles: • IT and business alignment • Capability builds around the services

	• Design the ICT system to meet sustainable requirements • Guarantee the information transparency and accessibility • Leverage the IT assets and component reusability • Maximise the interoperability by using common standard • Ensure the flexibility of the enterprise architecture to meet changing business needs and to leverage new technologies • Promote flexibility, agility and sharing of resources through virtualization • Maximise value through an outsource approach • Buy Commercial-Off-The-Shelf (COTS) software and services & interfaces delivered from public cloud commercial software-as-a-service providers if EUDPR compliant • Exploit existing platforms where fit-for-purpose and compliant • Organise IT system to increase the business process performance • Centralise data and applications. Furthermore, all technology selection and project scope should aim to increase the maturity of the 8 digital capabilities of EFSA's strategy: **Compute** Digital organizations make use of modern dynamic cloud-based service that allows for computation of code independent from the language and location of algorithms or data. This capability building is part of EFSA's development programmes and is aligned to the IT infrastructure ambitions of the Digital Commission through the AI Roadmap involving the Member States and in compliance with relevant EU Regulations and standards (incl. EUDPR/GDPR, (draft) EU AI Act). **Collaborate** A grid of interconnected communities that provide easy access to people and information, and that orchestrates heterogeneous community members. The projects that contribute to this capability align to the Commission's interoperability and cross-border principles. The projects will support the development of knowledge management capabilities that provide user-centric, data-driven and agile collaboration capability. **Knowledge Capture** Digital organizations capture formal and informal dialogue in such a way as to facilitate relationships across distributed knowledge pools. To automate and enhance the user-centric collaboration capability, IT tools (increasingly leveraging artificial intelligence) capture and monitor, and then proactively propose new collaboration opportunities, in alignment with and respect of information security standards and EU data protection rules and principles. **Talent Management**

	Digital organizations allow talent to create voluntary digital representations of themselves and other parties in order to facilitate connection and collaboration. Ensuring compliance with data protection principles, our projects and products supporting the competency and capabilities of experts, a much broader access to knowledge across the various European talent pools, established and emerging, and driving a more agile talent management require a shift from static taxonomic approaches to dynamic voluntary competency identification. **Ecosystem Management** Digital organizations create involuntary digital representations of organisations in order to assess capability, predict behaviour and leverage their capabilities. This digital principle is supporting the Commission openness and transparency principles, as well as the interoperability and cross-border principles. The projects that implement this digital capability will model the knowledge and competency of the competent authorities and other organisations we interact with. **Digital Dexterity** Digital organizations have digital dexterity. The cultural capability to be agile, multi-disciplinary, learning-focused and user-centered in all activity is an essential organisational component of the ability to leverage the digital capabilities and tools, and these are very much in line with the digital Commission enablers of digital leadership, enhanced governance and a stronger mandate for digital actors. The projects delivering the 2027 work programme address the change management and digital skill building that are needed to harness the tools of the new century. A&S and TP will consider the output of EPA Process 8.1 (Environment Scanning and Strategic Options Definition) A&S and TP will prepare the Target Enterprise Architecture (EA). The target EA will include the following domains: • **Target Business architecture**: describes the target state of the business capabilities and the business process model. • **Target Data Architecture**: describes the structure of an organization, existing logical and physical data assets and data management resources supporting the business process. • **Target Application Architecture**: describes what applications are in place to manage the data and support the business processes including their key components and interaction. • **Target Infrastructure Architecture**: describes what logical software and hardware capabilities and what networks providing communication paths are in place to support the business, data, and application services Based on the definition of the target EA, the **IT Plan** will be written by TS A&S outlining the path toward the target

	architecture state through a prioritised sequence of dependent software enablers which are to be implemented through EFSA development programmes and projects. EPA Process 12.1 will establish the programme and project portfolio that executes the IT Plan. Inputs to the IT Plan may also come from Process 8.1 Foresight and 7.1 Partnerships and contribute to new or modified IT needs through the EFSA strategic planning process.
Step 3	**3.0 Establish and review the IT Operational strategy in line with the EFSA IT roadmap and target Enterprise Architecture**
- Accountability Council (Accountable) - TS HoU (Responsible) - CORSER HoU - (Responsible) - DW (Responsible) - A&S (Responsible) - TP (Responsible) - DW (Consulted) - ISO/DPO (Consulted)	The **Preparedness Council** on **an annual basis** must establish or review the IT Plan and ensure its coherence with strategy and strategic processes (7.1 Partnerships, 8.1 Environment Scanning, 12.1 Strategy & Planning). The Preparedness Council will: • Decide on the adoption of the target EA and IT Plan prepared by TS (ref. step 4). • Analyse the Applications Portfolio to be in line with the business strategy • Review and endorse the proposals for the IT technology roadmap. • Decide on the decommissioning of technology if not aligned with technology roadmap. The **Accountability Council** on a **quarterly** basis must review IT service performance: • Identify and prioritise performance improvement initiatives in relation to service quality • Ensure EFSA's IT systems meet the needs of EFSA stakeholders and staff through the monitoring of service level agreements (SLA). • Provide recommendations on financial investments or financial savings to increase or decrease selected service level agreements (SLA). • Establish IT service performance targets and assign performance deviations • Ensure process performance and business case management through established corporate methodology for projects and process improvement initiatives. • Evaluate compliance to EUDPR requirements and ensure Data Protection Impact Assessments are duly performed when necessary.
Step 4	**4.0 Approval the IT Plan**

- Management Team – Preparedness Council - Chair - Executive Director - Participate - Heads of Department - Chair of Preparedness Council - Others on demand	The Management Team decides on adopting the IT operational strategy and technology roadmap proposed. Their decision may take into consideration the decision of the Accountability Council related to service and process performance gaps.
Step 5	**5.0 IT Plan updates**
- Accountability Council (Accountable) - Preparedness Council (Accountable) - Programme Managers (Responsible) - TS HoU (Responsible) - A&S (Responsible) - TP (Responsible) - DW (Consulted) - ISO/DPO (Consulted)	5.1 The **Preparedness Council** following a change of strategic objectives or targets, or changes in the work programme or partnerships, or based on outputs of 8.1 environment scanning and strategic options, asks TS (TP and A&S) to analyse the change's implications on the business process, Enterprise Architecture, and technology roadmap. 5.2 TS identifies possible impacts on Architectural Building Block (ABB) and Solution Building Blocks (SBB) of the new change of business strategy and business cases. 5.3 Process 8.1 Foresight and 7.1 Partnerships may provide requirements to be considered in the IT Plan update. 5.4 If no impact is identified, an Annex describing the update without change describes how the work programme and strategy changes are delivered without IT Plan changes. No further actions below follow in the event of no impact except for communication to the requestor(s). 5.5. TS (A&S and TP), with involvement of DW, ISO and DPO, produces an updated target EA and IT Plan and identifies financial, compliance and organisational impacts. 5.6 EFSA Programme Managers replan the revised IT Plan into the development projects through 13.2 Transformation Implementation Organising and chartering activities, applying PM2 methodologies for programmes. 5.7 The Accountability Council, taking into consideration the updates to the IT Plan and updated development portfolio plans with their financial and organisational impact, decides on the adoption of the updated technology roadmap as part of a revised development portfolio
Step 6	**6.0 IT Governance implementation**
- Management Team – Accountability Council - Accountable&Responsible) - Preparedness Council (Accountable & Responsible)	EFSA has adopted the COBIT framework for the governance of Information Technology. Based on the strategy of EFSA, the stakeholders' needs must be **evaluated** by identifying and agreeing on objectives to be achieved, must be directed by **prioritisation**, and must be **monitored** for performance against the objectives. EFSA has divided aspects of COBIT and

	good IT Governance into two councils, the Accountability Council and the Preparedness Council. The **Accountability Council** is responsible for implementing the following parts of the COBIT decision making framework: • Ensure that the governance approach is compliant with legal, contractual, and regulatory (i.e. EUDPR) requirements. • Ensure the cost-efficient delivery of solutions and services. • Ensure a reliable and accurate picture of service costs and likely benefits so that business needs are supported effectively and efficiently. • Ensure that IT risks to enterprise value are identified and managed, and the failures are minimised. • Propose the recommended IT service level agreement (SLA) balancing cost and performance • Ensure that adequate and sufficient IT-related capabilities (people, process, and technology) are available to support enterprise objectives effectively at optimal cost. • Review and endorse the proposals for the IT Plan. • Ensure EFSA's IT services and operational systems meet the needs of EFSA stakeholders and staff through monitoring of service level agreements (SLA). • Ensure that stakeholders are identified and engaged in the IT running services governance system (that the communication to stakeholders is effective and timely) EFSA has adopted the COBIT framework for the governance of Information Technology. Based on the strategy of EFSA, the stakeholders' needs must be **evaluated** by identifying and agreeing on objectives to be achieved, must be directed by **prioritisation**, and must be **monitored** for performance against the objectives. EFSA has divided aspects of COBIT and good IT Governance into two councils, the Accountability Council and the Preparedness Council The **Preparedness Council** is responsible for implementing parts of the COBIT decision making framework: • Ensure stakeholders' needs, conditions and options are evaluated to determine IT objectives. • Ensure a reliable and accurate picture of ex-ante project costs and likely benefits so that business needs are supported effectively and efficiently. • Ensures that IT-related decisions are in line with the enterprise's business strategies and objectives. • Set IT long-medium term strategy planning. • Review the target EA and IT Plan prepared by TS (ref. step 4).

	• Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change. • Recommend multi-annual financial ceilings for technology investment and organise task forces to study and propose selected topics within the remit of the Preparedness Council. • Ensure that stakeholders are identified and engaged in the IT governance system (that the communication to stakeholders is effective and timely) • Ensure that stakeholders are supportive of the IT strategy and road map. Ensure that stakeholders are supportive of the IT strategy and road map.
Step 7	**7.0 SOPs review**
- Accountability Council (Accountable) - TS HoU (Responsible) - A&S (Responsible) - TP (Responsible) - DW (Consulted) - ISO/DPO (Consulted)	Any change of one or more POTI dimensions may trigger a SOP(s) review. 7.1 Review SOP procedures according to the POTI dimensions. 7.2 Review the Project management methodology. 7.3 Approval of the new SOPs and Project management methodology.

ANNEXES

SOP Processes overview

The EPA macroprocesses of Enterprise Architecture (ref. EPA 13.1), Transform EFSA (ref. EPA 13.2) and Continuous improvement (ref. EPA 13.3) have been considered while defining the Standard Operating Procedures (SOPs). To better identify the interrelations with the EPA 3.0 processes and the other Units processes, the TS+Corser SOPs can be grouped and interrelated in 3 macro scenarios:

- ***Technological Advice (ref. EPA 13.1 Enterprise Architecture)***
- ***Project Implementation (ref. EPA 13.2 Innovation Implementation)***
- ***Compliance and Performance Improvement (ref. EPA 13.3 Continuous improvement)***
- ***Digital Services (ref. EPA 5.6)***

The figure below provides an overview of the SOPs and their interrelationships.