Digital Transformation in Higher Education

Critical Foundations

Citation

Hage, J., Zaroubi, T., & Jajeh, M. (2021). *Digital Transformation in Higher Education: Critical Foundations*. Digital Transformation Experts. Retrieved from https://dxexperts.pro/Assets/Publications/EN-US/DX-Higher-Education-Critical-Foundations-EN.

Revision 2021.12.10

TABLE OF CONTENTS

THIS PAGE WAS INTENTIONALLY LEFT BLANK

TABLE OF FIGURES

THIS PAGE WAS INTENTIONALLY LEFT BLANK

TABLE OF TABLES

THIS PAGE WAS INTENTIONALLY LEFT BLANK

Acronyms and Abbreviations

Abbreviation	Description
AB	Advisory Board
API	Application Programming Interface
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Planning
BoT	Board of Trustees
CDO	Chief Digital Officer
CDPO	Chief Data Protection Officer
CDTO	Chief Digital Transformation Officer
CERT	Cyber Emergency Response Team
CFO	Chief Financial Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
COOP	Continuity Of Operations Plan
CSOC	Cyber Security Operations Center
DAF	Digital Assurance Framework
DAG	Digital Assurance Group
DRP	Disaster Recovery Planning
DTSC	Digital Transformation Steering Committee
DTU	Digital Transformation Unit
DX	Digital Transformation
EU	European Union
GDPR	General Data Protection Regulation
HEI	Higher Education Institution
HESR	Higher Education and Scientific Research
ICT	Information Communication Technologies
IG	Institutional Governance
ISMS	Information Security Management System
ISO	International Standards Organization

Abbreviation	Description
ISRM	Information Security Risk Management
KPA	Key Performance Area
KPI	Key Performance Indicator
NDTS	National Digital Transformation Strategy
OECD	Organisation for Economic Co-operation and Development
OGP	Open Government Partnership
PMO	Program Management Office or Project Management Office
RACI	Responsible, Accountable, Consulted, and Informed
TQM	Total Quality Management
VP	Vice President

REMAINDER OF PAGE WAS INTENTIONALLY LEFT BLANK

INTRODUCTION

Digital Transformation (DX) is a series of significant, disruptive, and innovative culture, workforce, technology, and process changes coordinated and implemented across institutions to focus on student success, staff performance, education quality, and institutional competencies.

Digital transformation in the higher education sector across the world is implemented at different levels: (a) academia teaching and learning, (b) administration, and (c) research. The significance and effect of digitalization at all levels differ from one institution of higher education to another and from one country to the other. Nonetheless, it is a commonplace for most Higher Education Institutions (HEIs) that the main benefits of digitalization are increasing at an incredible pace as the higher education sector continues to embrace digital transformation, whether intentionally or unintentionally, as a means for survival and co-existence in the digital world (Brooks & McCormack, 2020).

The digital transformation strategy is built on five essential foundations: (a) Cross-Functional Governance, (b) Open Data, (c) Information Security Risk management, (d) Information Security Management, and (e) Business Continuity Management. The Digital Transformation Foundation and Pillars, as illustrated in **Figure 1**, must be considered at the sectoral level and led by the universities, central administrations, and other sectoral structures.

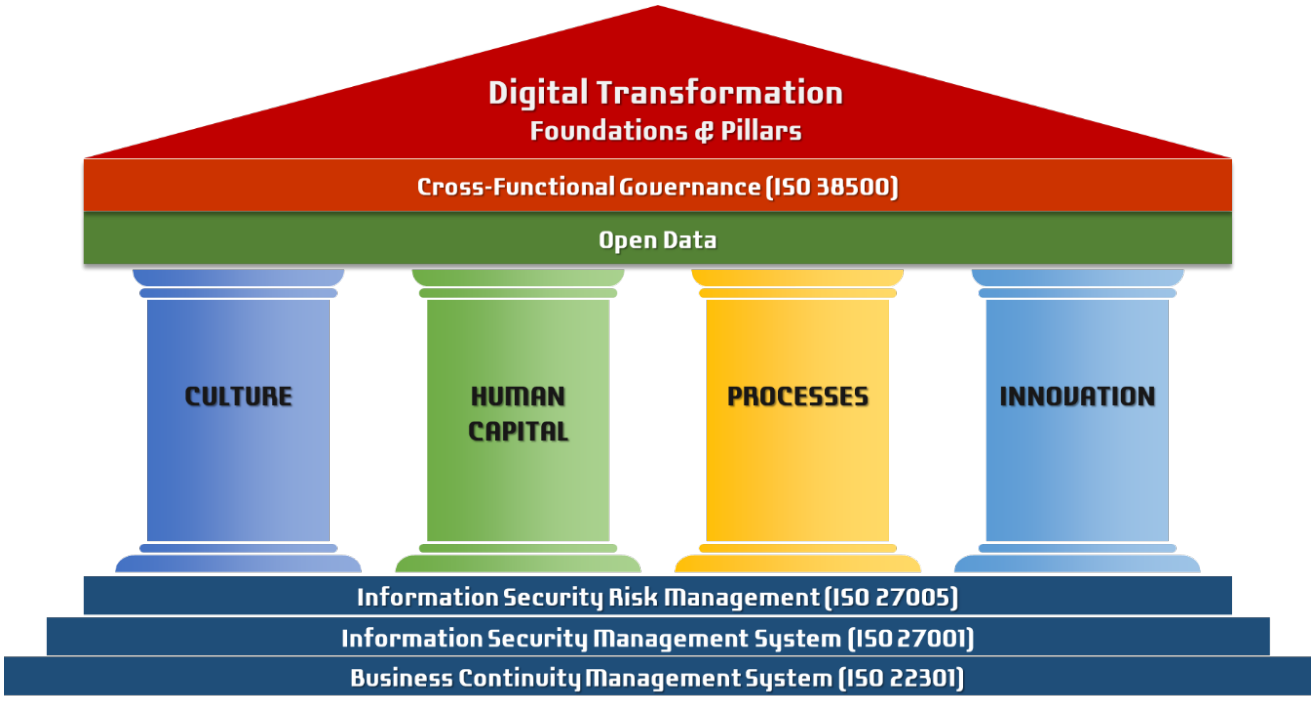

Figure 1. Digital Transformation Foundations and Pillars

Foundation 1. Cross-Functional Governance

Governance ensures that the higher education sectoral objectives are achieved by evaluating the needs of stakeholders along with options and conditions while (a) providing guidance for prioritization and decision-making processes; (b) monitoring progress and compliance; and (c) measuring performance against the stated strategic goal and objectives. Cross-functional Institutional Governance (IG) could be based on the ISO 38500 standard.

1.1. Governance Model

The governance model aims to promptly set the work, authority, ownership, and responsibilities and facilitate appropriate joint decision-making. The model helps anticipate and avoid problems that might arise before they have a significant impact on the roadmap set by the stakeholders. In addition, the governance model will guarantee priorities are set and no duplication of effort is taking place. The proposed model addresses three levels of governance determined by the technological and organizational maturity of the HEIs, which are included in the digital transformation implementation roadmap.

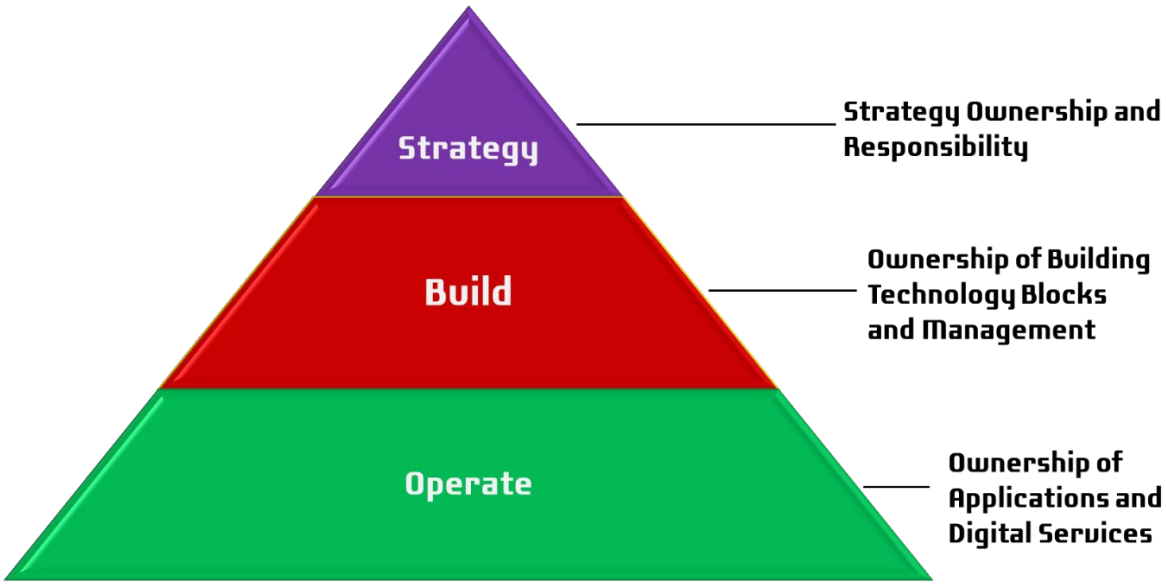

Figure 2. Governance Model

The three levels of the governance cover:

1. **Strategy Level** of governance covers the ownership of the Digital Transformation in Higher Education strategy. The strategy level will be responsible for all digital transformation initiatives' lifecycle, continuous improvement, and change management.

2. **Build Level** covers the ownership of the digital services and platforms' building blocks. It is responsible for designing digital services, platforms, and operations management building blocks.

3. **Operate Level** covers the digital services and platforms' integration, administration, and operations management.

1.2. Governance Composition Roles and Responsibilities

The below sections describe the model, roles and responsibilities, processes, structures, and reporting requirements that will enable parties participating in the digital transformational initiative in the Tunisian higher education sector to maintain an ongoing close, effective, and constructive relationship. Relationship-based partnerships with a clear delegation of responsibility are vital ingredients of success in every project. Such a governance model ensures high service levels and ongoing improvement and a strong, flexible, and mutually beneficial relationship between provider and recipient of service. The following six principles characterize the governance model and relationship among the parties:

Design Principle	Description
Proactive	The governance model ensures that decisions are made efficiently throughout the digital transformation projects by mitigating risks and anticipating problems before they occur.
Comprehensive	All activities within and surrounding the performance of the delivered solution, whether technological, administrative, or legal, will fall within the scope of this governance model.
Open	The governance model shall facilitate an open dialogue amongst the stakeholders at all levels of the relationship.
Shared	The governance model requires 'buy-in' from all parties and shall align the goals set in the digital strategy and implementation plan.
Flexible	Over time, stakeholders can review and modify the governance model as appropriate in response to changing requirements, e.g., new scope.
Collaborative	The governance model will provide a framework for close collaboration to build trust and respect amongst the stakeholders.

Table 1. Governance Model Principles

1.3. GOVERNANCE STRUCTURE

Governance shall be structured at four levels. The governance structure illustrated in **Figure 3** below will be headed by the most senior person at the sectoral level, the president of the HEI at the university level, or the director general at the entity level.

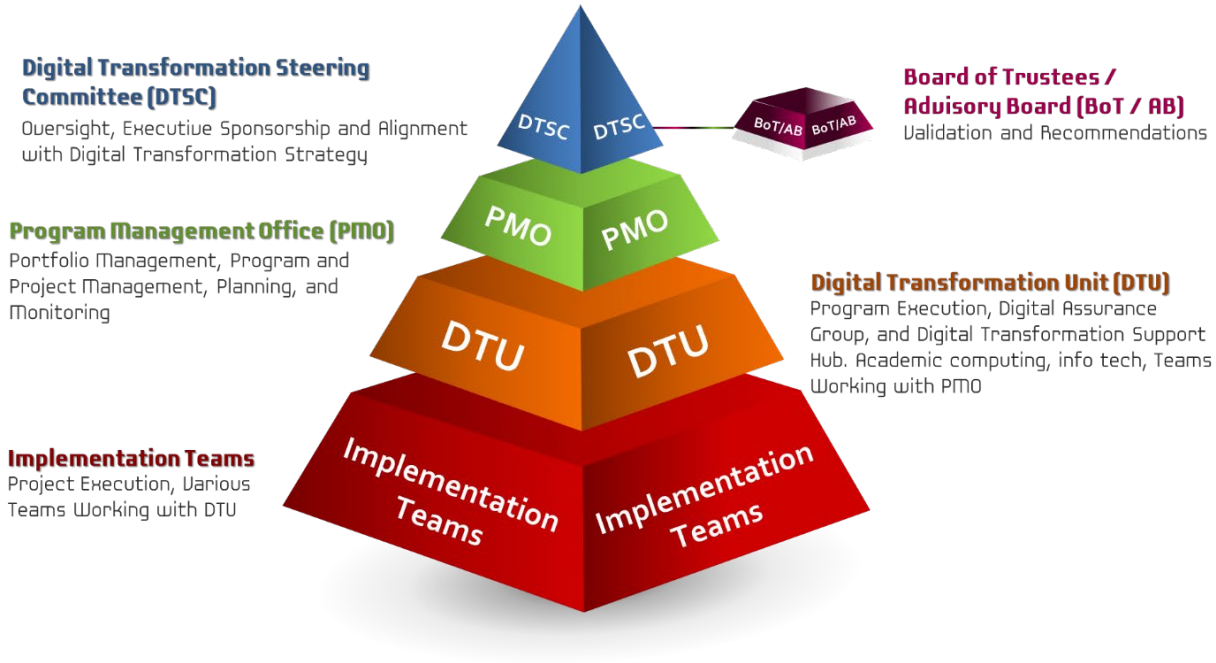

Figure 3. Governance Structure

The following matrix gives an overview of the structure and composition of each of the entities, committees, and teams within the governance structure and their respective roles and responsibilities:

Governance Body	Roles and Responsibilities
Digital Transformation Steering Committee (DTSC)	The Digital Transformation Steering Committee (DTSC) core function is to oversee all programs and projects in the DX Portfolio to ensure their alignment with the Digital Transformation in Higher Education strategy and goals, executive sponsorship, and the alignment with the National Digital Transformation Strategy (NDTS). The DTSC responsibilities are: • Define, develop, and update the Digital Transformation in Higher Education strategy and action plan and approve subsequent revisions

Governance Body	Roles and Responsibilities
	• Political and high-level commitment to the Digital Transformation in Higher education strategy vision and goals • High-level guidance and strategic decision making in alignment with the Digital Transformation in Higher Education strategy and action plan • Support and oversight of the overall Digital Transformation in Higher Education strategy plan including (a) Portfolio of Programs and Projects, (b) Priorities, (c) Budget, (d) Time Frame, (e) Resources, and (f) Key Performance Indicators (KPI) • Conduct periodic reviews of the overall status of the portfolio, programs, and projects delivered by the PMO and monitor their progress and alignment with strategic objectives • Manage potential interference by external influencers • Resolve escalated and complex issues, as necessary • Approve the project governance • Provide executive support for all digital transformation programs to increase chances of success and reduce resistance to change among the Higher Education Institutions • Ensure adequate funding is allocated for the various programs in the portfolio • Identify risks, issues, and dependencies, and find solutions to achieve the overall objectives and keep the programs on track • Obtain validation and recommendation on the Digital Transformation in Higher Education strategy and action plan from the Board of Trustees / Advisory Board (BoT / AB) • Coordinate with the Program Management Office (PMO) to ensure the proper support and standards are implemented across all portfolios, programs, and projects • Resolve conflicts as the PMO escalates them • Instruct the Audit Unit to conduct ad hoc or periodic audit functions

Governance Body	Roles and Responsibilities
	• Conduct bi-monthly meetings with the PMO to review project plans, statuses, and discuss escalations requiring intervention The DTSC is chaired by the senior national level person, e.g., Commissioner, Secretary, or Minister of Higher Education and Scientific Research (HESR), or a representative, and consists of senior leadership including: • President, Chancellor, Board of Trustees for Senior Leadership who should provide Senior Leadership commitment • Director Generals, Vice-Chancellor, COO, CFO, VP Administration/Human Resources for Administrative • Provost, Vice-Chancellor (Academic) for Academic Affairs • CIO, CTO, CDO for Technology • Vice-Chancellor/ Vice-Provost (Research) for Research and Innovation
Board of Trustees / Advisory Board (BoT / AB)	The members of this board are advisors from the education sector, including Trustees, Students (Student Government), Faculty (Faculty Senate), Employees (Employee Union), Alumni, and subject matter experts in the various fields. This group brings specific knowledge and skills that augment the knowledge and skills of the DTSC to guide the digital transformation journey effectively. The BoT / AB validates and recommends the strategy, portfolio, programs, projects, procedures, and processes to attain the required goals. The BoT / AB: • Does not have a formal authority to govern, and it can only offer advice, make recommendations, and provide vital information and materials • Plays a critical stakeholder engagement and public relations role • Provides a fresh perspective on programmatic issues • Serves as an essential complement to the effectiveness of DTSC as they carry out a specific initiative The BoT / AB responsibilities are:

Governance Body	Roles and Responsibilities
	• Supporting the DTSC in an advisory capacity • Advising the Program Management Office (PMO) and Digital Transformation Unit (DTU) on action plans
Program Management Office (PMO)	The PMO core function is managing the portfolio, programs, and projects and planning and monitoring to achieve the intended goals and successful outcomes. The PMO responsibilities are: • Conduct project feasibility and assessment • Survey all HEIs and collect requirements for digital transformation projects • Focus mainly on doing the appropriate work for the entire portfolio of digital transformation programs and projects compared to the PMO that focuses on doing the work right. Approve and submit projects for approval to the DTSC • Ensure all programs across the Higher Education Institutions are executed in unison to achieve the strategy set by the DTSC • Monitor portfolio and programs and measure the impact of the projects as they produce deliverables for providing feedback and ensuring continuous improvements • Coordinate and monitor program and project progress while ensuring alignment of the project implementations with the Digital Transformation in Higher Education strategic objectives • Produce guidance, standards, and best practices that help Digital Transformation Units (DTUs) with their digital transformation efforts across the project lifecycles • Support and provide program planning and prioritization of projects and activities • Manage the portfolio of programs to ensure their adequate alignment with the overall Digital Transformation in Higher Education strategy and oversight of program implementations to ensure their intended goals and successful outcomes

Governance Body	Roles and Responsibilities
	• Provide standard project management tools to support DTUs • Provide support mechanisms for cross-functional teams to integrate and use these tools • Provide training and facilitate project management, mentoring, and coaching • Provide support through local and international expertise for digital transformation projects • Support the development of right digital skills and culture to transform Higher Education services • Conduct post-mortems/capture, communicate and incorporate lessons learned • Provide change management, procedure simplifications, and process re-engineering • Support, develop and provide KPIs aligned with strategic objectives • Based on the request of the DTSC and a regular basis, conduct audit functions related to programs and projects: ▪ **Project Audit**: Timeline, deliverables, resources, risks, and issues. ▪ **Financial Audit**: Verify that projects are in line with budgets. ▪ **Legal Audit**: Ensure compliance to the national, sectoral, and institutional rules and regulations. • Report to the DTSC
Digital Transformation Unit (DTU)	The Digital Transformation Unit (DTU) is the Digital Transformation Support Hub, and its core function is program execution and digital assurance. The members of these units will be a mixture of specialists within each of the Higher Education Institution DX groups. Institutions will have a coordinator representing their HEI to coordinate with the DTU. The DTU responsibilities are: • Lead the technical implementations of the Digital Transformation in Higher Education

Governance Body	Roles and Responsibilities
	• Ensure standardization of shared digital-by-design e-services and common platforms to improve economies of scale and expedite delivery with the help of PMO • Coordinate and follow up on the progress of all the projects with DTUs established within other HEIs • Provide technical oversight over the various digital transformation tasks and activities • Provide technical oversight over implementation team • Provide Digital Assurance through Digital Assurance Group (DAG) • Escalate any significant issues or risks to the PMO
Implementation Teams	Formed of various thematic groups, the implementation teams' core function is project execution within their respective HEIs. These groups contain multiple teams working on many projects simultaneously. Each thematic group will have its role based on its expertise: • **The Legal and Organizational** Thematic group has the role and responsibility for coordinating all legal and organizational aspects of the digital transformation. Its responsibilities are: ▪ Participate in drafting necessary legal instruments and adjustments of existing ones ▪ Provide operational instructions ▪ Provide organizational adjustments ▪ Provide organizational change management • The **Technical** Thematic Group consists of project managers and similar profiles performing implementation and related activities as part of the overall effort. Their responsibilities are: ▪ Implement projects within their corresponding HEIs ▪ Coordinate all related activities ▪ Synchronize inter-related tasks to reach common goals and facilitate communication with external stakeholders and institutions when needed ▪ Coordinate the development of training programs and training of affected employees ▪ Report to the DTU, regularly and frequently

Governance Body	Roles and Responsibilities
	▪ Escalate any critical issues or risks to the DTU ▪ Facilitate the approval and endorsement of key deliverables

Table 2. Roles and Responsibilities of Governance Bodies

1.4. Portfolio Management Structure

The implementation plan of the **Digital Transformation Strategy in Higher Education** shall consist of a portfolio of programs, with each program consisting of one or more projects owned by the national entity and various HEIs, and with each project varying in complexity and scope. It is advisable to run a program for each Key Performance Area (KPA).

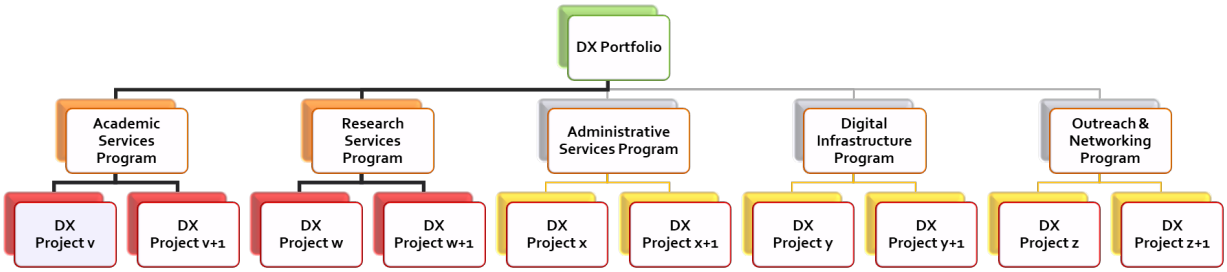

Figure 4. Portfolio, Programs, and Projects Relationship

Portfolio, Program, and Project management will adhere to standard Portfolio Management Framework principles. It will abide by the strategic goals set by the Digital Transformation in Higher Education Strategy and implementation plan approved by the DTSC. Strategic goals are the responsibility of the Digital Transformation Steering Committee (DTSC).

Portfolio, program, and project management is the responsibility of the Program Management Office (PMO), whereas program execution is the responsibility of the Digital Transformation Unit (DTU). Project Execution is the responsibility of an individual or combined implementation team. **Figure 5** below depicts the recommended portfolio management structure.

1.5. Project Management Structure

Project execution is the responsibility of the Implementation Teams, who are the project owners. The counterparts of the implementation teams are members of the Digital Transformation Unit. The Program Management Office (PMO) supports all the implementation teams by being the hub for all programs and projects. The DTU will

execute some tasks, e.g., standard integrated and interoperable platforms, unified login, and open interoperability platform.

The Audit Group will perform ad hoc and periodic audit functions based on the instructions of the Digital Transformation Steering committee.

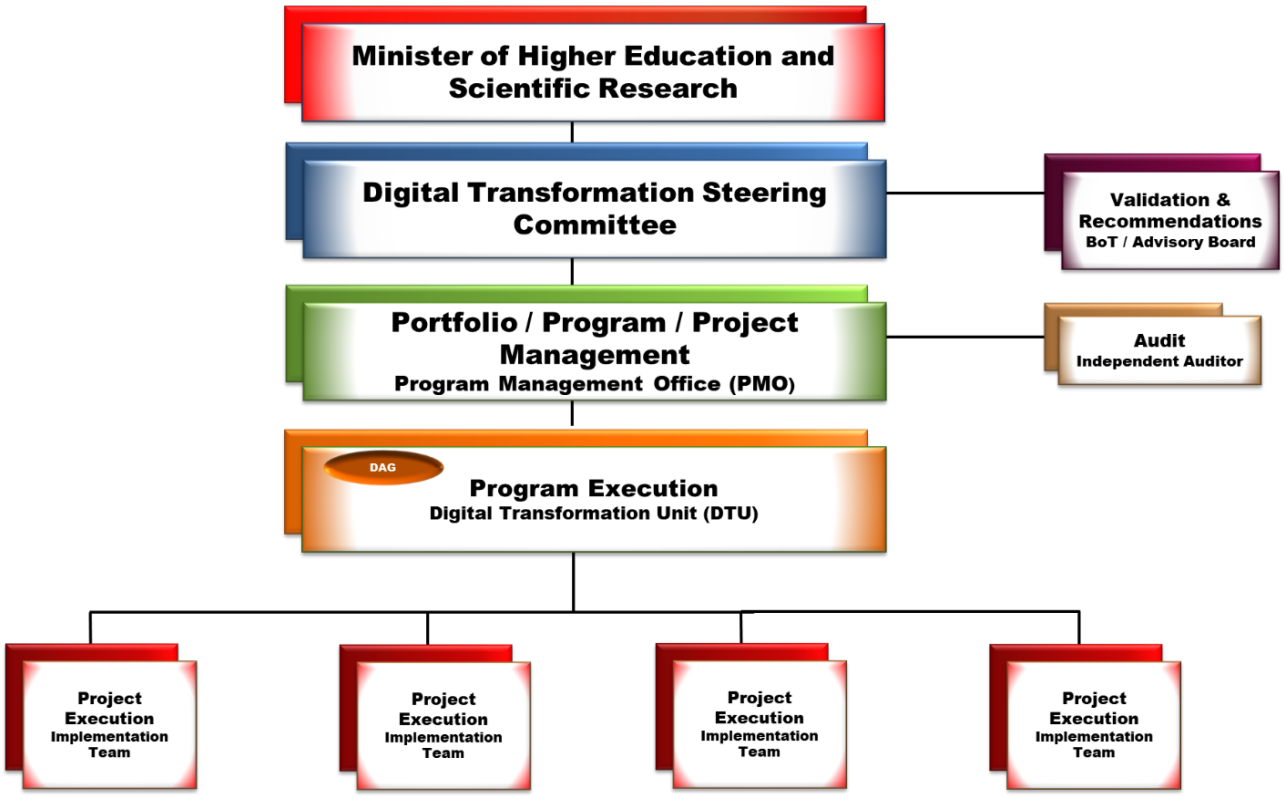

Figure 5. Portfolio Management Framework

1.6. DIGITAL TRANSFORMATION UNIT

The Digital Transformation Unit (DTU) will be a virtual entity consisting of digital experts residing in the HEI and a fusion of specialists with technology, management, quality assurance, legal, and communication backgrounds. The DTU will be the catalyst for digital transformation and for co-creating innovative ways of doing things in the higher education sector. The DTU will assume ultimate responsibility for the user experience and advocate modern approaches to delivering student-centered services.

The DTU will have specialized knowledge hubs that operate horizontally across higher education. Strategic focus areas include technology, data, digital services, cybersecurity, laws and regulations, business process re-engineering, and digital skills. In addition to the DTU specialists, the knowledge hubs bring together expertise in strategic areas from various higher education institutions and harness their talents to enable synergy in solutions to common problems across the higher education sector. The DTU must institute the roles of a Chief Digital Transformation Officer (CDTO) and a Chief Data Protection Officer (CDPO) in each of the digital transformation units.

1.7. Governance of Inter-Institutional Services

Each transformed digital service will have an empowered service manager accountable for it. When the service uses APIs to access data from the national higher education entity, various HEIs, general directorates, and other governmental organizations and data providers, the data owners will control the security of the APIs. All the relevant data owners will formally authorize appropriate security privileges at the design stage of the digital service. The service manager shall work closely with the DTU team on data classification and the interoperability platform.

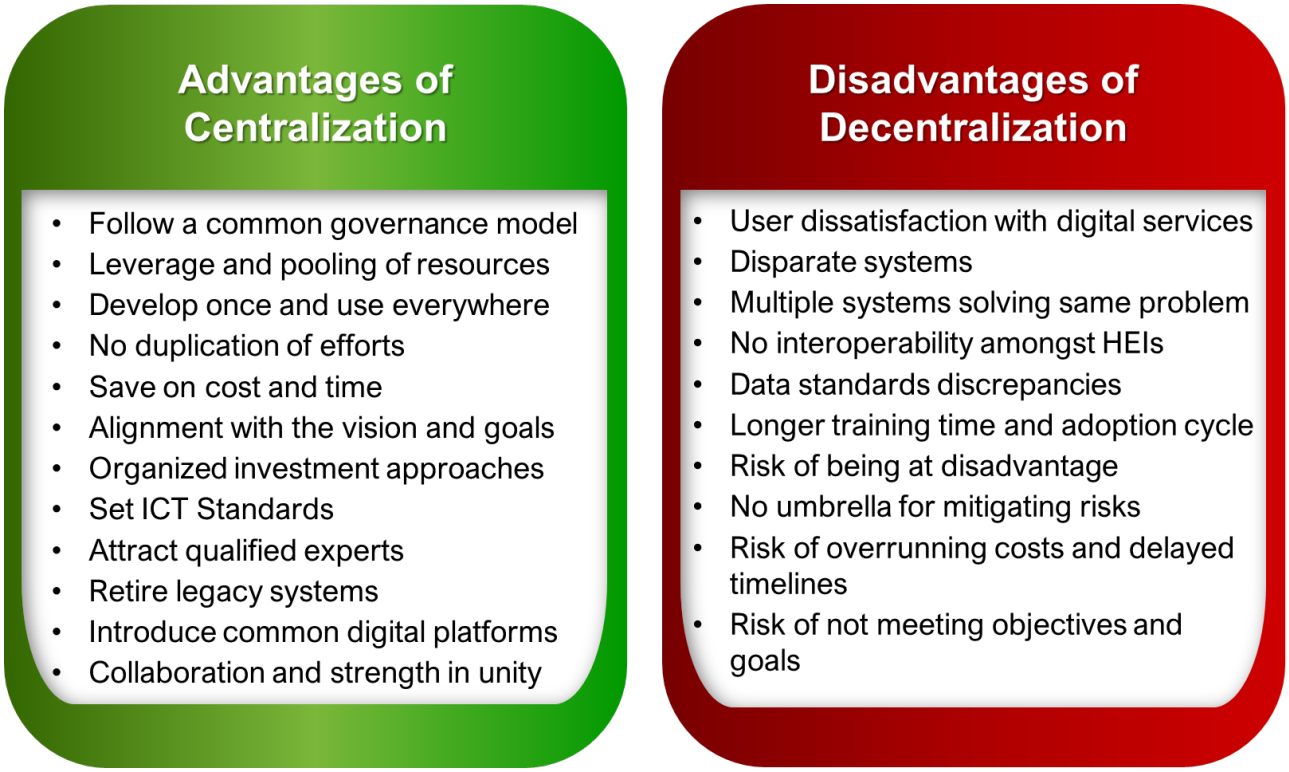

Figure 6. Centralization vs. Decentralization of Digital Services

1.8. Responsible, Accountable, Consulted, and Informed (RACI) Matrix

With responsibility comes accountability; therefore, with each role and activity within the governance model, stakeholders will be responsible, accountable, consulted, or informed (RACI) for specific decisions and actions. The following are the definitions of the four RACI components:

Responsible: The role that performs the work to complete a task or decide. There shall be at least one role responsible, although others can be delegated to assist in the necessary work or decision. Responsibility can be shared among multiple parties.

Accountable: The ultimately answerable role for the adequate and successful completion of the deliverable or task. This role ensures the task's prerequisites are met and delegates the work to the responsible function(s). In other words, an accountable role must approve the work that the responsible position performs. Unlike responsibility, accountability cannot be shared; thus, there must be at least one, and only one, role specified as Accountable for each task or decision.

Consulted: The Consulted role comprises stakeholders whose opinions are sought – typically subject matter experts and entities affected by the tasks performed and decisions made – and with whom there is two-way communication.

Informed: This role consists of the entities who must be kept up to date on the progress, often only on the completion of the task or deliverable, and with whom there is just one-way communication.

Figure 7. RACI Framework

The **Responsible, Accountable, Consulted, and Informed (RACI) Matrix** helps identify roles and assign cross-functional responsibilities to deliver the strategic goals of the digital transformation strategy.

1.9. Monitoring and Reporting

Regular reviews shall occur among the parties to ensure the alignment of activities among the relevant levels of the governance structure. An overview of such proposed meetings is provided below:

Frequency and Type	General Topics Covered
Digital Transformation Steering Committee (DTSC) Progress Review – Bi-Monthly	• Review meetings are held every two months • High-level status of portfolios, significant deliverables, and milestones • Review of significant risks and issues • Resolution and mitigation strategies for critical issues and risks • Decisions related to the overall direction of programs • High-level strategic coordination with external stakeholders • Organize ad hoc meetings of the PMO, on short notice, based on significant events and or risks that call for strategic decisions and coordination among the stakeholders • Audit reviews
Program Management Office (PMO) Management of Programs – Bi-Weekly	• Portfolio coordination meetings are held every two weeks • Coordination with external stakeholders • Make sectoral and strategic decisions that have a potential impact across several work efforts and project groups • Programs coordination meetings are held every two weeks • Review items achieved previously and plan for next period • Synchronize interdependent activities and plans • Review and discuss potential issues and risks • Coordination amongst DTUs • Progress reviews on projects • Make technical decisions that have a potential impact across several work efforts and project groups

Frequency and Type	General Topics Covered
Digital Transformation Unit (DTU) Project Coordination Meeting – Weekly	• Project coordination meetings are held weekly
Implementation Team Meetings	• Project team meetings shall be organized among the individual teams and according to each team's needs

Table 3. Monitoring and Reporting Activities by Governance Entity

1.10. Total Quality Management (TQM)

As the institution embarks on its digital transformation journey, significant changes and continual improvements must be implemented across the entire institution. Fear of change often leads to a halt in sharing ideas and a loss of improvement opportunities. Operational excellence and the cultural transformation that must accompany it constitute critical foundational elements for a successful digital transformation that delivers value to the education sector, including Trustees, Students, Faculty, Employees, and other stakeholders.

1.10.1. Digital Assurance

There are serious concerns that the traditional approach to provisioning ICT assurance is fragmented, resulting in unnecessary duplication of efforts, waste of investment, inefficiency, delay, non-interoperability, security breaches, lack of proper governance, and failure. There should be a continual evaluation of the risks associated with digital transformation projects.

1.10.2. Digital Assurance Group

The Digital Assurance Group (DAG) will be set up within the Digital Transformation Unit (DTU) to provide coordinated assurance oversight of all significant ICT and digital investment projects across the Higher Education sector. This group will develop a standardized process and a more rigorous governance model to oversee the HEI's investment in ICT projects. The group can provide greater transparency and optimization of the investment portfolio by developing a strategic investment analysis, benefits management, governance, risk management, and program management.

The Digital Assurance Group will coordinate with the Digital Transformation Steering Committee on cybersecurity legislation and with chief information officers of the various HEIs to improve existing cyber legislations, address legal issues that concern the sector, and keep pace with international developments. The Digital Assurance Group will focus on forging ongoing strategic partnerships to provide independent assurance and improved benefits delivery for institutions and people using the digital services online. The group will be a focal point for legal advice on transforming existing paper-based business processes into innovative digital ones.

1.10.3. Digital Assurance Framework

In consultation with the CIOs of HEIs, the group will establish a Digital Assurance Framework (DAF) and a supporting tool to help its implementation and enable cross-institutional project reporting. The framework will improve strategic alignment and assurance for digital projects across the project life cycle by implementing a risk-based process embodying best international practices. The framework's purpose is to ensure that HEI's ICT projects are aligned with the national digital transformation strategy and delivered on time and budget.

The DAF sets out digital project reporting processes and assurance requirements, including mandatory due diligence reviews, health checks, deep-dive reviews, and project status reporting. The DAF is designed to deliver:

1. Improved service delivery for citizens
2. Value to the institutions
3. Greater return on ICT investment
4. Reduced risk
5. On-time and on-budget delivery
6. Standardized metric-driven project status

The DAF shall apply to all in-flight ICT projects and those about to commence or are planned for the next financial year and have an estimated cost above a certain threshold.

1.11. Operations

The Operations Group focuses on the efficient day-to-day execution of live services, such as Web hosting and maintaining Websites; running common digital platforms; monitoring cloud service level agreements; responding to security incidents, analyzing user feedback, and improving system performance. In addition, the Operations Group shall manage all relevant projects, such as communications and digital awareness campaigns and procurement processes. The portfolio of the projects varies in substance, size, and quantity from time to time to reflect the priorities of the relevant period.

Foundation 2. Open Data

The Organisation for Economic Co-operation and Development (OECD) encourages countries to join its Open Government Partnership Program (OGP). Complying with the national open data policies and plans, if they exist, is vital. The higher education sector and the HEIs shall develop their adequate open data policy and strategies in consultation with the national entity responsible for the sector.

Foundation 3. Information Security Management System

All information held and processed by an organization is subject to vulnerabilities inherent in its use and threats of attack, error, and acts of God, e.g., flood, fire, or other natural disasters. Information is generally considered an asset, which has a value requiring appropriate protection against the loss of availability, confidentiality, and integrity. Enabling the availability of accurate and complete information promptly to those with an authorized need is a catalyst for institutional efficiency. The Information Security Management System (ISMS) shall be based on the ISO 27001 standard.

Security must be embedded into all applications as the first line of defense. To achieve such a level of protection, all actors in the higher education sector must adopt the Security-by-Default approach, whereby the security controls embedded in every digital service are set at the highest levels of protection, by default. One of the hallmarks of being more proactive in securing data is that protection is the default posture. In other words, the ISMS should be Secure-by-Design.

By using such standards, organizations can develop and implement a framework for managing the security of their information assets, including financial information, intellectual property, student records, employee details, and information entrusted to them by other stakeholders or third parties. As per the ISO Standard 27001, any organization must establish, implement, maintain, and continually improve an Information Security Management System (ISMS), following the requirements of this international standard. The ISMS uses a framework of resources to achieve an organization's objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources. Information security involves applying and managing appropriate security measures to consider a wide range of threats, intending to ensure sustained business success and continuity while minimizing the impact of information security incidents.

3.1. Cybersecurity

Cybersecurity addresses substantial risks that could potentially affect the HEIs, while at the same time, acting as a key enabler for delivering immensely improved digital services. Confidence in the cybersecurity measures and transparency in the use of personal information are vital for gaining stakeholders' trust and attracting them to transact online. Cybersecurity presents a significant challenge for the higher education sector. Usually, there is a national agency charged with implementing the general rules on the protection of information systems and network security.

It is highly recommended for the national-level organization, e.g., ministry, department, or commission, to take the lead on behalf of the higher education sector to work with other national agencies and entities involved in defining and implementing the national cybersecurity strategy. It is nearly impossible to take a sectoral approach to this complex endeavor. The national entity is responsible for implementing and operating a nation-wide Cyber Emergency Response Team (CERT) to respond to cyber threats and managing a Cyber Security Operations Center (CSOC) to collect and share cyber-threat

intelligence, monitor real-time digital operations, identify cyber risks, and execute mitigating actionable plans in response. For the higher education sector, the national entity shall define a cybersecurity policy that will support the national cybersecurity strategy.

3.2. Data Protection and Privacy

Data privacy is not achievable without data protection, and one cannot have data protection without information security. Digital transformation projects create new risks as technology implementers must deal with personal data, classification, protection, and data security. The data protection and privacy laws give individuals the right to:

- access all personal data concerning them;
- correct, complete, rectify, update, modify, clarify, or delete when the data is inaccurate, equivocal, or when its processing is prohibited;
- object, at any time, to the processing of personal data concerning them for valid, legitimate, and serious reasons, except where the treatment is planned by law or is required by the nature of the obligation; and
- prevent personal data from being shared with third parties for advertising purposes.

Although the EU's General Data Protection Regulation (GDPR) Law was intended for its member states, the law has an important impact on foreign universities outside the EU. If students were on vacation in the European Union, visiting their university's website outside the EU requires their HEI to comply with the privacy laws of the GDPR in the handling and processing of information and data belonging to these students (European Union, 2016). The compliance requirements include consent, authorization, and protection of individual information. Because the ethical use of data is an increasingly important topic of discussion among the OECD member states, the HEIs shall institute a data ethics framework regulating the purposes for which data are used and the tools and techniques that enable stakeholders to maintain control over their data (Van Ooijen, Ubaldi, & Welby, 2019). The EU's GDPR is the gold standard for assuring the highest level of data privacy. Most prominent of the GDPR is the Right to be forgotten or the Right to erasure, whereby individuals have the Right to request organizations to delete their personal data.

Foundation 4. Information Security Risk Management

Information security is achieved by implementing an applicable set of controls, selected through the chosen risk management process, and managed using an ISMS, including policies, processes, procedures, organizational structures, software, and hardware to protect the identified information assets. The ISO Standard 27005 for Information

Security Risk Management (ISRM) is used for assessing, mitigating, and managing risks, including (a) Risk Identification, (b) Risk Analysis and Evaluation, (c) Risk Treatment, and Acceptance, and (d) Risk Monitoring. These controls are specified, implemented, monitored, reviewed, and improved, where necessary, to ensure that the specific information security and business objectives of the actors in the higher education sector are met.

Relevant information security controls are expected to be seamlessly integrated with the various processes. It is essential for the higher education sector to note that a whole sectoral strategy for information security risk management must be considered to highlight how it is applied at the different sector levels. Internal stakeholders, namely the central administration, universities, and others, should have an overall top-level view of the higher education system.

Foundation 5. Business Continuity Management System

Business Continuity Planning (BCP) focuses on maintaining business operations with reduced or restricted infrastructure capabilities or resources. If the higher education sector's ability to perform its mission-critical work tasks is maintained, BCP can manage and restore the environment. If the continuity were broken, business processes would stop, and the sector would enter disaster mode.

Business Continuity Management (BCM) aims to provide the sector with the ability to respond effectively to threats, such as natural disasters or data breaches, and protect the organization's interests. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management, and contingency planning. According to the ISO 22301 Standard, a Business Continuity Management System (BCMS) emphasizes the importance of:

- Understanding continuity and preparedness needs and the necessity for establishing business continuity management policy and objectives.
- Implementing and operating controls and measures for managing overall continuity risks.
- Monitoring and reviewing the performance and effectiveness of the business continuity management system.
- Continual improvement based on objective measurements.

5.1. Continuity of Operations

All actors in the higher education sector must create fault-tolerant systems and redundant data storage so that sensitive data is maintained through an emergency. These entities must also invest in redundant hardware systems so that an office can still function if a local site is compromised. Continuity of operations planning involves developing individual processes and applications to continue directly after a crisis.

The Continuity of Operations Plan (COOP) establishes policy and guidance to ensure that critical functions continue while personnel and resources are relocated to an alternate facility in case of emergencies. The sectoral and institutional continuity of operations plan must consider the budgets required to maintain the availability of any service provided to stakeholders, including the required cost of operations for all data systems and information security systems, which keep those systems operational.

5.2. Resilience and Disaster Recovery

Disaster Recovery Planning (DRP) steps in where Business continuity planning (BCP) leaves off. When a disaster strikes and a business continuity plan fails to prevent interruption of the higher education sector's activities, the disaster recovery plan kicks in. It guides the actions of emergency-response personnel until the end goal is reached, which is to see the affected digital services restored to total operating capacity in their primary operations facilities. The disaster recovery plan must be set up to run on autopilot almost.

The DRP is designed to reduce decision-making activities during a disaster as much as possible. Essential personnel shall be well trained in their duties and responsibilities in the wake of a disaster and must know the steps they need to take to get the sector up and running as soon as possible. To recover operations with the most outstanding possible efficiency, the sector's actors must engineer their disaster recovery plan to recover those functions and services with the highest priority. Therefore, critical systems must be identified and prioritized to determine the tasks and order to restore after a disaster or failure.

Resilience and disaster recovery in digital transformation are generally seen as operating costs rather than value drivers. Although organizations invest a lot into system availability, new digital technologies are considered drivers of value, while resilience and disaster recovery are viewed as expenses rather than investments. However, meeting operational KPIs and preventing technology disruptions are very closely linked. It is essential to consider how other areas, such as resilience, must be transformed when undergoing a digital transformation. Poor resilience means that all the benefits of new technology could be undone because of the high costs of recovery, damage to reputation, loss of revenue, and loss of data.

REFERENCES

Brooks, D.C., & McCormack, M. (2020). *Driving Digital Transformation in Higher Education*. ECAR research report. Louisville, CO: ECAR, June 2020.

European Union (2016). General Data Protection Regulation. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Van Ooijen, C., Ubaldi, B., & Welby, B. (2019). A data-driven public sector: Enabling the strategic use of data for productive, inclusive, and trustworthy governance. *OECD Working Papers on Public Governance* (33). doi:10.1787/09ab162c-en

REMAINDER OF PAGE WAS INTENTIONALLY LEFT BLANK

THIS PAGE WAS INTENTIONALLY LEFT BLANK