Disaster Resilience in Higher Education Systems via a Cloud University Model

WORK PACKAGE 3

ACTIVITY 3.2

TITLE: Analysis of Partner HEIs

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA).

Basic project information

Project title	**Disaster Resilience in Higher Education Systems via a Cloud University Model**
Acronym	**CLOUD HED**
Project number	**2024-1 AT01-KA220-HED-000249632**
Start	October 2024
End	September 2026
Website	www.cloud-hed.eu
Project team	WPZ Research GmbH, Austria Sumy State University, Ukraine Ben Gurion University of the Negev, Israel Riga Technical University Rezekne Academy, Latvia National Agency for Higher Education Quality Assurance, Ukraine Cardinal Stefan Wyszynski University, Poland Tel-Hai College, Israel

Research Design

Assessment of level of preparedness / status quo analysis

- RQ1: What is the current level of preparedness of partner HEIs for transitioning to an emergency-induced cloud-based university model in terms of:
    - RQ1.1: management structures?
    - RQ1.2: teaching conditions, practices, and curricula?
    - RQ1.3: technical and infrastructural requirements?

Identification of (HEI-specific and general) key requirements

- RQ2: What are the key requirements for implementing an emergency-induced cloud-based university model in terms of:
    - RQ2.1: management structures?
    - RQ2.2: teaching conditions, practices, and curricula?
    - RQ2.3: technical and infrastructural requirements?

Potential institutional challenges and mitigation strategies

- RQ3.1: What institutional challenges and opportunities can be identified for shifting towards an emergency-induced cloud-based university model?
- RQ3.2: How can the institutional challenges and opportunities be addressed to ensure a smooth transition?

OVERVIEW

Below is the completed analysis grid (raw data). The final analysis can be found in Régent et al. (forthcoming), *Building the "Cloud University": Institutional Readiness for Emergency Digital Transformation in European Higher Education*.

DIMENSION	RQ1: Level of Preparedness	RQ2: Key Requirements	RQ3:	
			Challenges	Mitigation Strategies
Management Structures	-Varied levels of centralization/ decentralization -Presence of Digital Tools and Platforms for Management Functions -Reliance on Physical Documents and In-Person Meetings	-Matrix structure -Specific training of management personnel for cloud-based transition -Comprehensive investments and upgrades	-disrupted communication channels (power/internet instability) -delayed decision-making -data fragmentation due to non-integrated tools -Security risks	-Training, Support, Orientation -Procedural changes
Teaching Conditions, Practices, Curricula	-Levels of operational flexibility and preparedness: between moderate and high -varied teaching models, but online models are present across all HEIs -Varied levels of faculty digital literacy -SSU has Internal Center for Professional Development for regular training, workshops, and certification programs for digital literacy and pedagogical skills -Partial availability of modular courses and micro-credentials among HEIs	-Clear communication protocols and management responsibility upon cloud shift -Cloud design operations support -Market research -Integration of resilience and transversal skills -Common platform for research activity -Modernize assessment strategies	-Need for stronger Digital equity -Assessment strategies need to be more robust -Absence of clear communication protocols and spheres of management responsibility -Resilience skills and transversal skills integration are low-medium -Varied digital literacy -Inconsistent adoption of tools -Micro-credentials are not yet widely implemented	-Investing on further digital platforms (especially for research and assessment), and digital pedagogy -Structured and tiered digital literacy program and training with role-specific training, regular refreshers, and incentives for participation to address faculty proficiency gaps -Stronger communication protocols -Leveraging departments for cloud shift

DIMENSION	RQ1: Level of Preparedness	RQ2: Key Requirements	RQ3:	
			Challenges	Mitigation Strategies
	-Need for further integration of transversal and resilience skills		-Maintaining student engagement	-Conduct market research to identify and adapt to new physical environments that support cloud-based operations -expanded IT support -virtual academic advising, and psychological support -Establish and enforce emergency teaching protocols, data privacy and security policies -Strengthen assessment strategies
Technical and Infrastructural Requirements	-varied level of up-to-date digitalization properties -Adopted cloud platforms vary -Addressing digital divide through: TEL-HAI: laptop loan programs, subsidized internet access, on-campus IT labs SSU: free access to online platforms, energy-independent resources Redundancy procedures present in TEL-HAI and SSU Need for more robust disaster recovery protocols Cybersecurity measures are present but need further developments	-Substantial investment for upgrades and cloud transition -Digitalizing modules for cloud -Forming typical business processes scheme -Migration of core systems (ERP, HR, Finance, Student information systems) -Upgrades: Redundancy procedures, High speed network -Cybersecurity enhancements -Unified platform strategy with SSO	-Digital Divide -requires significant data migration and integration efforts for cloud transition -Complexity on forming standardized business process scheme -Bandwidth and network reliability may not support sustained high-traffic cloud operations during emergencies -software licensing and platform integration -Cybersecurity gaps	-Significant investments (as per SSU: 6 million euros a year) -Continuous digitalization of modules -Phased roadmap for cloud migration -Expansion on programmes for filling gaps from digital divide -Continuous role-specific training for IT, faculty, and staff -establishing a dedicated Digital Transformation Office or Task Force

1.1. Dimension: Management Structures

This section analyses the current status, digital integration, and adaptability of the management structures of Tel-Hai Academic College (TEL-HAI), Sumy State University (SSU), Cardinal Stefan Wyszyński University in Warsaw (UKSW), and Riga Technical University (RTU) Liepaja / Rezekne, focusing on their preparedness for potential cloud-based transitions and emergency scenarios.

HEI	RQ1: Level of Preparedness	RQ2: Key Requirements	RQ3:	
			Challenges	Mitigation Strategies
SSU	"well-defined governance structure" balances centralized strategic leadership with decentralized operational autonomy hybrid governance model Extensive use of digital tools in management functions	Specific training of management personnel for cloud-based transition Implementation of a matrix structure for departments in a cloud-based transition	Management structure is not flexible in eliminating positions or departments Potential Resistance: Cloud Transition Impact on Control Information Flow in a Crisis: Delayed Decision-Making Dependence on Internet Connectivity Cybersecurity vulnerabilities Adaptation of staff to new systems under pressure	Flexibility could be provided through the matrix structure of departments in a cloud-based transition Orientation: centralized monitoring of cloud platforms to foster sense of control in managers Orientation: Cloud systems allow real-time access to documents and data from any location and easily accommodate growing data and user needs during crises.
Tel-Hai	-relatively centralized management structure -some operational functions exhibiting decentralization -Presence of Crisis Management Team -Integration of a variety of digital tools and platforms for management functions gradually reducing its reliance on physical documents and in-person meetings	-targeted training and structured support for: -Technical skills, Communication Protocols, new workflows and procedures -Comprehensive investments and upgrades	-Current digital systems are fragmented and not fully integrated -Continued moderate reliance on physical documents and in-person meetings Cultural dependence on in–person interaction among senior leadership and admin staff	A shift to a comprehensive cloud-based model is proposed to significantly enhance integration, data centralization, and remote operability -Streamlining this transition towards a fully digital, cloud-supported model is crucial for boosting agility and continuity. Significant procedural changes and staff training

HEI	RQ1: Level of Preparedness	RQ2: Key Requirements	RQ3:	
			Challenges	Mitigation Strategies
			Prevalence of physical paperwork and signatures for contracts, financial approvals Siloed data integration, lack of workflow standardization Compromised internet connectivity Inconsistent user adoption or poor training can lead to inefficiencies	
UKSW	Semi-decentralized decentralization is considered beneficial during emergencies Platforms for communication and planning are used The institution demonstrated adaptability during the COVID-19 pandemic	-need for digitalization is widely acknowledged -aims for secure communication and shared access within its management structure Specific training and support for management personnel Cybersecurity protocols Scenario-based drills Substantial investment is recommended in infrastructure, faculty training, cybersecurity, and AI-driven platforms	Reduced Control Need for increased coordination and flexibility for the transition	Systems need to be user-friendly
RTU	Digital platforms used for employee communication, data storage	N/A	N/A	N/A

1.2. Dimension: Teaching Conditions, Practices, and Curricula

This section analyses the current status, digital integration, and adaptability of the management structures of Tel-Hai Academic College (TEL-HAI), Sumy State University (SSU), Cardinal Stefan Wyszyński University in Warsaw (UKSW), and Riga Technical University (RTU) Liepaja / Rezekne, focusing on their preparedness for potential cloud-based transitions and emergency scenarios.

HEI	RQ1: Level of Preparedness	RQ2: Key Requirements	RQ3:	
			Challenges	Mitigation Strategies
SSU	-high level of operational flexibility -employs a diverse and flexible educational model: (face-to-face, blended, online modalities) -proprietary internal platforms, MIX for managing the educational process -Examination for MOOCs and online assessments -Use of Google Workspace (Classroom, Docs, Meet), Zoom, Microsoft Teams, and Turnitin Level of faculty digital literacy is moderate to high -Has Internal Center for Professional Development for regular training, workshops, and certification programs for digital literacy and pedagogical skills -Modular courses and micro-credentials available. -Technical and digital skills in curriculum are at a medium level -Transversal skills: medium level -Resilience skills: low level	-Develop and implement clear communication protocols and define spheres of management responsibility for shifting teaching and learning to the cloud during an emergency -Needs cloud design operations support -Requires market research for new physical environments to support a cloud-based university model -Improve incorporation of resilience skills in the curriculum beyond the current low level -Establish a common platform for research activity as currently there is none -Modernize assessment strategy processes beyond mostly manual document forming with KPIs	-No common platform for research activity -Assessment strategy is provided mostly by forming documents with KPIs by hand, indicating a manual and potentially inefficient process -resilience skills at a low level -absence of clear communication protocols and defined spheres of management responsibility	-Implement comprehensive cloud design operations support to facilitate a smooth transition -Conduct market research to identify and adapt to new physical environments that support cloud-based operations -Stronger communication protocols for cloud-based university operations during emergencies -Leverage the Internal Center for Professional Development to enhance training for faculty and staff on cloud-based operations, digital content creation, and potentially, integrating resilience skills more explicitly into pedagogy -Invest in or develop integrated digital platforms to support research activities and automate assessment strategies

Tel-Hai	-moderate to high level of preparedness -employs a hybrid teaching model: face-to-face instruction, blended learning, and online modalities (both synchronous and asynchronous) -Faculty utilize a range of digital systems (Moodle, Zoom, Microsoft Teams, Panopto, Google Workspace tools. -Assessment: TomaTest, Moodle quizzes, plagiarism detection tools -AI-powered tool “Courseophia” for curriculum design -Growing selection of modular courses and flexible learning option -Microcredentials being discussed	-Expand modular course offerings, -Formalize micro-credential pathways -Digital learning environment integration -Embed resilience as defined, assessable skill across all programs -Develop a curriculum-wide framework to formalize and assess transversal competencies -Requires reliable cloud platforms (e.g., Microsoft Azure, AWS, Google Cloud) that are integrated with existing tools like Moodle, Microsoft 365, and ERP systems -Needs device and connectivity support through loan programs or subsidies for students and staff, especially during displacement or outages -Fortify cloud-based backup and recovery tools -Expand digital helpdesk with real-time troubleshooting, multilingual support, and extended service hours during crises	-Full teaching flexibility is limited in programs requiring physical presence -Digital literacy varies significantly among faculty, with some senior staff less comfortable with newer platforms -inconsistent adoption of tools, gaps in training for advanced features or pedagogy-focused tech usage, limited time for faculty to attend training, and a lack of standardization across departments -Formal micro-credentialing is not yet widely implemented -Digital equity and access: not all students or faculty have equal access to reliable internet, updated devices, or quiet learning environments -Pedagogical readiness varies, with some faculty struggling to redesign practical or lab-intensive courses for online delivery -Maintaining student engagement and mental health is more challenging in a fully remote model, especially during a crisis	-Continue investing in digital pedagogy and cloud-supported tools to expand the adaptability and inclusiveness of its teaching model -Implement a structured, tiered digital literacy program with role-specific training, regular refreshers, and incentives for participation to address faculty proficiency gaps -Investment in training, infrastructure, and digital inclusion strategies -faculty training on cloud tools, online pedagogy, assessment strategies, and resilience in digital classrooms -expanded IT support, including real-time troubleshooting and extended service hours during crises -virtual academic advising, mental health services, and tutoring accessible through cloud platforms for student support -Develop digital learning materials and secure online assessment tools to support remote learning -Establish and enforce emergency teaching protocols and data privacy and security policies

		-development of cloud-accessible digital learning materials like video lectures and interactive modules -secure platforms for online exams, plagiarism detection, and alternative assessment formats suited for remote learning -predefined emergency teaching protocols covering communication, attendance, and grading flexibility -clear data privacy and security policies aligned with regulations like GDPR		
UKSW	-moderate level of preparedness -adopted hybrid and online teaching models -Flexible assessment methods, such as open-book exams and oral defences, along with modular learning pathways, are emphasized -focusing on emergency teaching and the use of digital tools, and digital proficiency among faculty varies -training includes trauma-informed practices -adopts modular learning, micro-credentials, and flexible certification options to support crisis learning and alternative pathways	-More specific details are needed on the software and systems used by teaching staff -Clarity is required on the exact online platforms used for teaching activities and whether they are integrated across various functions like communication, lectures, and assessment -Strong cloud infrastructure is required to support a cloud-based emergency scenario -Further development and support for asynchronous and mobile learning	-While online platforms are used, their exact systems and integration status across different teaching functions remain unclear -lack of access to necessary resources and unequal digital readiness among faculty members -digital access inequality among students and staff -readiness for online delivery in practice-based fields and addressing mental health issues that arise during emergencies	-Emphasize and enhance faculty training, including specific programs on trauma-informed practices to address the psychological impact of crises -Address digital access inequality by providing alternative or offline learning options for vulnerable groups -Invest in and ensure strong infrastructure to accommodate increased demand during emergencies -comprehensive psychological support for students and staff to address mental health issues during crises

	-Online platforms are broadly used for communication and emergency instruction, including mobile learning and remote collaboration	-Requires adequate psychological support for students and staff during emergencies -Revised assessments and inclusive policies to ensure quality and continuity of education in a cloud-based emergency scenario		-Revised assessments and inclusive policies to ensure the continuity and quality of education in a cloud-based emergency scenario
RTU	N/A	N/A	N/A	N/A

1.3. Dimension: Technical and Infrastructural Requirements

This section illustrates the current situation of the technical and infrastructural readiness of Tel-Hai Academic College (TEL-HAI), Sumy State University (SSU), Cardinal Stefan Wyszyński University in Warsaw (UKSW), and Riga Technical University (RTU) Liepaja / Rezekne. The analysis focuses on the preparedness of the HEIs for potential cloud-based transitions and emergency scenarios.

HEI	RQ1: Level of Preparedness	RQ2: Key Requirements	RQ3:	
			Challenges	Mitigation Strategies
SSU	-high level of digitalization (particularly on learning process) Utilizes own LMS and hardware, cloud services (Google Workspace, Microsoft Azure). -High level of IT infrastructure redundancy and reliability -Addresses digital divide by providing free access to online platforms for all students and staff and possesses energy-	-form a typical business processes scheme for universities -Digitalizing other activities and interconnected modules that are not yet in the cloud	-Complexity of forming a standardized business process scheme that can apply broadly across universities, given their inherent differences in organizational structures, communication methods, and interaction rules	-University's strategic approach involves continuing to digitalize its remaining activities and interconnect modules -Estimated investment for a basic cloud transition is approximately 6 million euros for one year.

HEI	RQ1: Level of Preparedness	RQ2: Key Requirements	RQ3:	
			Challenges	Mitigation Strategies
	independent resources for servers to ensure continuity during power outages -Easy-to-scale infrastructure for typical cloud decisions -Data protection: all information is copied multiple times to different media and servers, with network insurance -Cybersecurity measures: Cloudflare (network filter) -40 modules of university activity into the cloud			
Tel-Hai	-functional and moderately up-to-date -not yet optimized for large-scale, long-term, cloud-based operations -utilized partial cloud adoption through Microsoft OneDrive, Teams, and SharePoint -no full institutional migration to major cloud platforms -utilizes centralized on-premises servers for core systems like ERP and data storage, along with Microsoft Office 365 for communication and productivity, and Moodle as its primary Learning Management System (LMS) -IT infrastructure: moderate redundancy (local backups, some mirrored services)	-migration of core systems (ERP, HR, finance, student information systems) to cloud platforms like Microsoft Azure or AWS -High-speed network and redundancy upgrades -Investments in automated cloud-based disaster recovery and backup systems with real-time syncing and geo-redundancy -Cybersecurity enhancements (e.g. endpoint protection, encrypted cloud storage, MFAs for user accounts, security audits and incident response planning.	-reliance on legacy systems and on-premises dependencies (requires significant data migration and integration efforts for cloud transition) -Bandwidth and network reliability may not support sustained high-traffic cloud operations during emergencies -lack of scalable disaster recovery infrastructure -software licensing and platform integration -Cybersecurity gaps	-demonstrated strong adaptability during past emergencies (like COVID-19 and recent wartime conditions) -A phased roadmap for cloud migration of core systems is required -an expansion of hardware lending programs, subsidized connectivity, and accessibility tools (e.g., screen readers, captioning) is needed to ensure equitable access -continuous, role-specific training for faculty and staff in cloud-based systems, online pedagogy, data security, and digital workflow management is crucial

HEI	RQ1: Level of Preparedness	RQ2: Key Requirements	RQ3:	
			Challenges	Mitigation Strategies
	-disaster recovery protocols are not yet robust -Laptop loan programs available, subsidized internet access, on-campus computer labs -Current software licenses may have user caps that limits simultaneous access	-Unified platform strategy with SSO -Scalable licensing models	-Digital divide (limited proactive outreach to students)	-establishing a dedicated Digital Transformation Office or Task Force responsible for planning, coordinating, and evaluating cloud implementation across departments, supported by a dedicated budget and executive-level oversight
UKSW	-Need for robust IT infrastructure -IT software, hardware, networks: N/A -Cloud readiness varies across institution (Needs further detail)	Substantial investment for infrastructure upgrades, faculty training, cybersecurity enhancements, implementation of AI-driven platforms (Needs further detail)	-Digital gaps -Scalability limitations -Cybersecurity concerns (Needs further detail)	AI, blockchain and decentralized platforms as potential responses -Substantial investments (Needs further detail)
RTU	N/A	N/A	N/A	N/A

GAPS and NEXT STEPS (GENERAL)

Gaps emphasized by partner HEIs		Next steps (for Guidelines)	Output
Management and Organization	1. Fragmented Digital Management Systems	Develop and enforce integrated digital management platforms; digitize all workflows and records.	Guideline section on digital management platforms.
	2. Insufficient Training for Leadership and Staff	Implement role-specific, recurring cloud competency and leadership training programs.	Guideline section on leadership training programs
	3. Resistance to Change	Launch change management initiatives; communicate benefits and engage early adopters as champions.	Guideline section on the cloud university model advantages to promote support
	4. Absence of Standardized Procedures	Establish and disseminate cloud governance protocols and digital workflow standards.	Guideline section on cloud governance protocols
Teaching, Curriculum, and Faculty Gaps	1. Varied Digital Literacy Among Faculty	Tiered, regular digital skills training; incentivize ongoing learning.	Guideline section linking to digital skills training for faculty.
	2. Limited Integration of Resilience and Transversal Skills	Update and integrate curricula	Guideline section focusing on instructions for curriculum revision
	3. Inconsistent Adoption of Digital Tools	Select and mandate common digital tools, providing training and centralized support.	Guideline section on the use and consistent adoption of digital tools
	4. Assessment and Student Engagement Challenges	Develop standardized cloud-based assessment tools and student engagement protocols for remote learning.	Guideline section for cloud-based assessment and student engagement protocols

Gaps emphasized by partner HEIs		Next steps (for Guidelines)	Output
Technical and Infrastructural Gaps	1. Outdated or Fragmented IT Systems	Prioritize full migration of legacy systems; phase out obsolete platforms; ensure integration and interoperability.	Guideline section for the cloud migration process
	2. Digital Divide	Expand device loan programs, subsidized connectivity, and digital inclusion support for vulnerable groups.	Guideline section for promoting digital inclusion
	3. Cybersecurity Vulnerabilities	Strengthen cybersecurity frameworks: multi-factor authentication, regular audits, staff/student awareness training.	Guideline section for ensuring cybersecurity
	4. Incomplete Disaster Recovery and Redundancy Protocols	Implement cloud-based disaster recovery protocols with geo-redundancy and frequent drills.	Guideline section for cloud migration drills and protocols
	5. Complexity in Data Migration and Integration	Develop phased migration roadmaps; budget for system compatibility, data cleansing, and support during transition.	Guideline section for the cloud migration process
General Strategic and Policy Gaps	1. Unclear Cloud Transition Roadmaps	Create detailed, phased migration strategies including milestones, risk ownership, and feedback mechanisms.	Guideline section for the cloud migration process
	2. Regulatory and Compliance Challenges	Establish a compliance committee to monitor regional/global data regulations and guide cloud provider selection.	*Guideline section for committee structuring
	3. Resource Allocation and Funding	Secure dedicated budget lines for training, infrastructure, and support; regularly review funding needs.	*Guideline section for funding and allocation