

What do good digital services look like in a research-intensive University?

Dr Simon Brownsell
IT Director of Strategy and Change

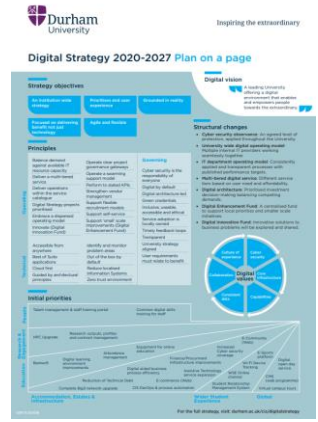
GridPP47

23rd March 2022

“A leading University offering a digital environment that enables and empowers people towards the extraordinary”

1. An institution wide strategy
2. Prioritises end user experience
3. Grounded in reality
4. Focused on delivering benefit not just technology
5. Agile and flexible

You can now watch the animations here:



Projects

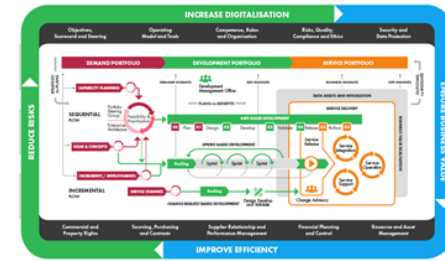
	21/22				22/23				23/24				24/25+			
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Digital Campus	CAFM - Computer Aided Facilities Management				Timetabling & Room Booking				Digital Signage				Access Control Standardisation			
	Flexible Working				Campus Analytics				Smart Car Parks				Robotic Automation			
					Accommodation Management				Physical Security Enhancements				Smart Utilities			
Digital Education	Equipment for Online Learning				Pilot to Production Digital Learning				Digital Exam/Assessment/Marking							
	VLE DUO to Ultra + Decommission				Lecture Capture Enhancement											
	Learning Support (Virtual)															
Digital Experience	WSE Online				Open Day Digital Service				Commercial Partnerships				Personalised AI Student Coach			
	Virtual Campus Tours												Digital School Outreach			
									Digital Preservation							
	LMS Replacement				Enhanced Content for Alumni								AI Supported Digital Careers Service			
	E-commerce												WiFi City Partnership			
	VR Student/Staff Recruitment				Digital Durham Award				E-Sports							
					Assistive Technology Service Expansion											
	Finance & Procurement															
Digital Foundations – Data	Analytics & Reporting Platform								Social Listening							
	Mobile App															
	Master Data Management															
Digital Foundations – Skills	Common Skills for Staff								Specialist Skills for Research				Digital Skills for Community			
	Digital Learning/Edu Skills												AI Enhanced Recruitment			
	Digital Learning				Talent Management											
Digital Foundations – Sustainability	Reduction of Technical Debt & Cyber Security															
	Internet				IT Dept DevOps & Automation				Realtime Digital Infrastructure Reporting				Role Based Access			
									Identity & Access Management				Next Generation Web			
									IPVS				Upgrade Data Centres			
Digital Research	Research Outputs & Profiles				Research Data Management				Secure Research Data Environment				Experiment Automation			
					High Speed Research		Single Ethics System						VR/AR for Research			
					HPC Upgrade								Big Data Processing Service			
					Digital Support for Research								AI Fund Matching			
					Research Impact Module								AI Research Contracts			
													REF Module			
Student Systems Improvement	Creating an Integrated Student Experience (CISE)															
	Pre-Enrollment (PNE)				Student Feedback System											
					Student Absence Management											

Structural reform

1. Agree Strategy projects and deliver according to University governance
2. Agree and implement a University wide Cyber strategy
3. Agree and implement a University wide operating model
4. Enhance the CIS operating model
5. Improve data management and data standardisation
6. Identify and deliver innovation
7. Support smaller scale projects
8. Enhance digital KPI's and measurement
9. Improve Coms and Engagement

What do we need from an operating model?

“In both culture and technology, universities are one of the most **open and outward facing sectors**. This enables and eases collaboration between academics across borders, and is likely a key component of their success. **Unfortunately, this also eases the task of an attacker.**” National Cyber Security Centre, Sept 2019



www.managebt.org

Cyber security

- A moral imperative
 - Harm to individuals
 - Profits going to organised crime
- Financial loss
- Legal implications
- Operational disruption
- Loss of valuable intellectual property
- Reputational damage
- Missed opportunities

Business continuity

- Student expectations
- Service operations

Education

- Reliable and consistent IT
- Performant IT

Research

- Enable innovation
- Performant IT
- Sustainable

Operating model considerations

Model	Description	Cyber security	Business continuity	Support teaching	Support research
Central	<i>Central control for IT decisions and delivery</i>	Strong (unless drive behaviour underground)	Strong	In most cases	Only where conforms to repeatable examples

“Freedom in a framework”

DITO – Distributed IT Operating

“To **embrace** the benefits of a dispersed IT operating model that provides specialist and timely local IT expertise to facilitate world leading teaching, research and local business processes. The operating model should be **sustainable** with appropriate investment, **minimising single points of success**, and **apply data and cyber security controls consistently** across all University IT providers.”

**One IT service (appropriate levels of performance/risk)
operated by multiple internal providers**

- A **vision**
- Assurance that **roles and responsibilities** are understood
- Assurance that **cyber controls** are appropriate and effective
- Effective IT **business continuity** throughout the dispersed operating model

DITO – Roles and responsibilities

- Adopting our cascade governance model re H&S
- Locally operated IT services are defined
- Responsible officers are accountable for locally operated IT
- Local services adhere to University controls (single risk appetite)
 - Cyber security controls
 - Architectural principles and standards
 - Operating principles (i.e. support, recovery, procurement)
- Oversight and risk escalation (identification of themes, agreed mitigations)
 - Local responsibility
 - DITO board level
 - University board (CIO and SIRO)
- Audit (self assessment, internal and external assurance)

Risk Matrix

Severe	5					
Major	4					
Moderate	3					
Minor	2					
Insignificant	1					
		1	2	3	4	5
		Very unlikely	Unlikely	Moderately possible	Very likely	Almost certain

DITO – Cyber controls

- Technical controls – all working to the same risk appetite
 - NIST Security and Privacy Controls for Information Systems and Organisations (800-53)
 - 1,190 → 105

Control	All systems	High risk data	Critical system	Publicly accessible
The system is routinely scanned for vulnerabilities, using an up-to-date scanner	A	M	M	M
Media containing confidential data are marked according to the University's Information Classification and Handling standard	A	M	A	A

DITO – Cyber controls

- Technical controls – all working to the same risk appetite
 - NIST Security and Privacy Controls for Information Systems and Organisations (800-53)
 - 1,190 → 105
- Communications
 - Alerting service
 - CoP - Technical
 - CoP – Organisational cyber and data champions
- Managed SOC (detection and response)
- Cyber training
- University IT cyber service catalogue
- Explore a dedicated research environment

What do good digital services look like in a research-intensive University?



Durham
University

Crossing the Chasm



Questions?

