

The background of the entire page is a dark blue, futuristic digital landscape. It features a grid of glowing lines and numerous small, scattered characters and symbols, including binary code (0s and 1s) and various alphanumeric characters, creating a sense of data flow and digital connectivity.

Digital Strategy

2020-2023

CONTENTS

Introduction	3
Strategic Review and Solutions	5
2018 Digital Strategy Review – GAP Analysis	6
Cyber Security	7
Enterprise Application Review and Strategy	9
Service Model	11
Service Offer	12
Solutions	13
The Plan (Stabilise, Optimise and Transform)	14
Conclusion	15

INTRODUCTION

This document sets out a refreshed Ulster University Digital Strategic vision and plan for 2020 to 2023. It details how a newly formed Digital Services directorate will provide technical, digital, information and application strategies to underpin the operational running of the University, whilst enabling transformation and growth.

It recognises the fundamental change brought about by COVID and the need to develop solutions to support greater mobility in a secure, sustainable, and agile manner. Including the greater use of cloud and managed services, remote solutions and standardised platforms, and the centralisation of procurement and support services.

All of which requires a refreshed operating model and solution set, with a cultural shift that focuses on partnerships, collaboration, and shared outcomes across all corners of the University.

It builds upon principles and ambitions outlined within the 2018 Digital Strategy based upon 'empowering people through digital', and provides staff and students access to enabling technologies and digital services across a range of foundation infrastructure and end user platforms, both in a localised, cloud, and mobile manner.

The ambition is the delivery of robust, scalable, resilient and performant applications and infrastructure. With technology solutions that enable access to information at the right time, in the right setting, on the right device, in context, and in a secure way.

This vision will be enabled by building upon existing strategies, structures, technologies, processes, and relationships, whilst implementing best practice ways of working and taking advantage of new and emerging solutions. Some will require investment, though we will redirect existing funding where possible to meet these objectives.

Through the lens of a staff member a newly formed Digital Services will be highly visible, engaged, supportive, responsive, and always professional in our approach. Service reporting will be improved, and our work will be based upon the use of best practice in areas of service management, process, governance, and policy. We will operate as a trusted partner to the university and be a strategic enabler.

For the student, the digital journey needs to be seamless with greater emphasis and focus placed upon their Digital wants, needs, and requirements. This is our intent.

Points discussed within this Digital Strategy are:

- Need to stabilise, optimise, and transform existing service offer and solution set.
- Deliver against recommendations identified through the 2018 Digital Strategy.

- Provide best in class foundation infrastructure, end user compute technology, and digital services capability.
- Adopt 'best practice' standards, frameworks, and processes to assure service quality.
- Redefine the service and application solution set.
- Deliver a robust Cyber Security programme to protect the University against Cyber-attack.
- Place our staff and students at the core of everything we do, and delight in service delivery.
- Become a trusted and fully engaged partner across all functions of the University estate, including the student population, and wider sector.

Key to which is re-branding of the Information Services Division (ISD) to Digital Services, building a new model of working, re-defining the service offer, and stabilising the existing technology and digital estate.

In delivery we work in a spirit of partnership and collaboration and develop a more formalised approach to service delivery. We will develop and propose a centralised approach to standardisation and procurement of technology assets and review the funding model needed to ensure sustainability and growth within the Digital estate.

This Digital Strategy is based upon a three-point plan.

- Stabilisation, 'fixing what is broken'.
- Optimisation, 'leverage what is already in place'.
- Transformation, 'design, develop and build a new service delivery model and long-term application and information strategy'.

STRATEGY REVIEW AND SOLUTIONS

Review existing technology and application solution sets, including service offer, the organisational structure, infrastructure, digital, technical, information and application estate, and cyber security controls and plans.

Whilst some technology sets in use are current others are aged and in need of upgrading or replacing, this is known as the 'technical debt' and will be reviewed as part of the 'stabilisation' phase of this Digital Strategy.

Historically technical and digital solutions have been procured in a decentralised manner whereby standardisation was difficult to achieve, and for these environments Digital Services have limited, or no, oversight or control. This poses a potential Cyber security threat and will be addressed as part of 'stabilisation', and within the Cyber programme.

Elements of Cyber Security technical controls are in place though not always centrally managed or delivered in a unified way. This poses a significant risk and could, if left unattended, result in system loss, data loss, financial loss and reputational damage to the University. This will also be addressed through 'stabilisation', and within the Cyber programme.

In doing so Digital Services will positively engage stakeholders to:

- Review, rationalise and develop enabling infrastructure, commodity technology platforms and applications required to support digital transformation and enable new ways of working.
- Develop and promote solutions to consolidate and standardise solutions sets.
- Listen to staff and students and develop services that promote delivery of information at the right time, in the right setting, on the right device, in context, and in a secure way.
- Build trust and confidence in the work that we do, and service we provide. Digital Services will become a trusted advisor and strategic partner to all functions of the University, and externally across the sector.
- Develop a robust approach to Cyber Security preparedness and incident response.

We will do this in a way that reflects our values and behaviours and ensures Digital Services, and Ulster staff and students have access to highly available infrastructure, information, digital, applications and technology services.

This will be enabled through:

- Leveraging existing investment in infrastructure and technology platforms.
- Implementation of modern teaching and learning solutions and technology infrastructure.

- Implementation of commercially focused sourcing strategies.
- Development of digital partnerships and working with partners to design and deploy solutions that are scalable across the Higher Education economy.
- Investment in Cyber Security.
- Focus on staff and student user experience.

In doing so Digital Services will:

- Review existing services and develop a well-constructed and clear service catalogue, including details on service criticality, service response, and service support.
- Review all Enterprise Applications and work to develop a future applications road map.
- Develop and deliver a robust Cyber Security programme.
- Listen, engage, and deliver.

2018 DIGITAL STRATEGY REVIEW – GAP ANALYSIS

The road map included within the 2018 Digital Strategy outlined a series of ambitions, deliverables, and outcomes across each of the strategic themes. Although no timeline was placed upon delivery, phasing was based upon a three-point approach, i.e., Now 'Baseline', Soon 'Transitional' and 'Future' Strategic.

Digital Services will work to review each deliverable and engage with stakeholders to ascertain their current and future state. This will be undertaken in conjunction with the applications review, outputs from which will inform the future application strategy and road map.

CYBER SECURITY

A pan-university approach to dealing with the Cyber threat is required, as is investment for assessments, training, accreditation, tooling, and dealing with the 'technical debt'.

Digital Services do not view Cyber Security as a like to have, but a must have, we recognise the continual threat and response required to mitigate against attack whilst ensuring adequate planning, monitoring and development of Emergency Preparedness and Disaster Recovery processes are maintained. This remains a key and constant element of this Digital Strategy.

A University wide Cyber capability review is required, with the outcomes used to develop remedial plans for priority areas and the development of business cases to mitigate risk. Digital Services will work towards attaining Cyber Essentials and Cyber Essentials Plus accreditation. This is a Government backed, industry supported scheme to help organisations protect against common online threats.

This is an important first step as vulnerabilities to simple attacks could mark Ulster out as target for more in-depth attention from cyber criminals. Cyber Essentials will provide peace of mind that our defenses will protect against most of common cyber-attacks, simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.

Upon achieving Cyber Essentials, we will move towards the more rigorous certification level known as Cyber Essentials Plus.

As the Higher Education sector is becoming a direct target of Cyber Criminals, and with high-profile attacks occurring we will develop tactical and strategic plans to mitigate against the Cyber threat into a formal Cyber Programme, and use dedicated and experienced subject matter experts, with external support to improve levels of Cyber defense and preparedness. This will include the development of a dedicated Cyber function led by a Chief Information Security Officer (CISO).

In progressing our Cyber plans Digital Services will follow the advice, guidance, and resources available through the National Cyber Security Center (NCSC), The Joint Information Security Committee (JISC), the Information Commissioner Office (ICO), Universities and Colleges Information Systems Association (UCISA), and others.

A model proposed by the NCSC which is a core requirement of Cyber Essentials Plus is known as the '10 Steps to Cyber Security' (Figure 1). This is, and will continue to be, used to measure our Cyber maturity, and develop our longer-term Cyber plan.

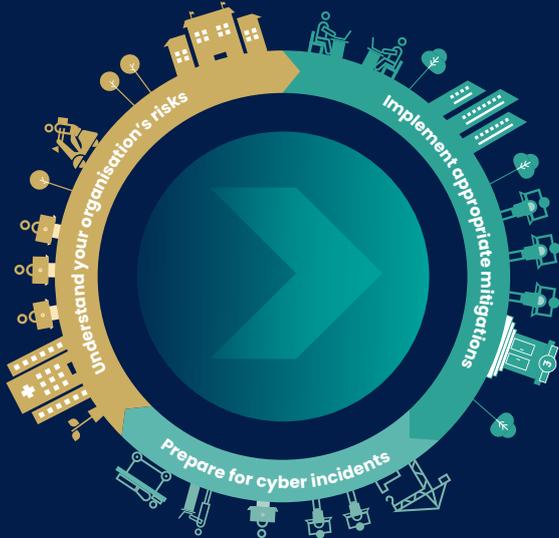
FIGURE 1: National Cyber Security Centre, 10 Steps to Cyber Security



10 Steps to Cyber Security

This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.

- **Risk management**
Take a risk-based approach to securing your data and systems.
- **Engagement and training**
Collaboratively build security that works for people in your organisation.
- **Asset management**
Know what data and systems you have and what business need they support.
- **Architecture and configuration**
Design, build, maintain and manage systems securely.
- **Vulnerability management**
Keep your systems protected throughout their lifecycle.

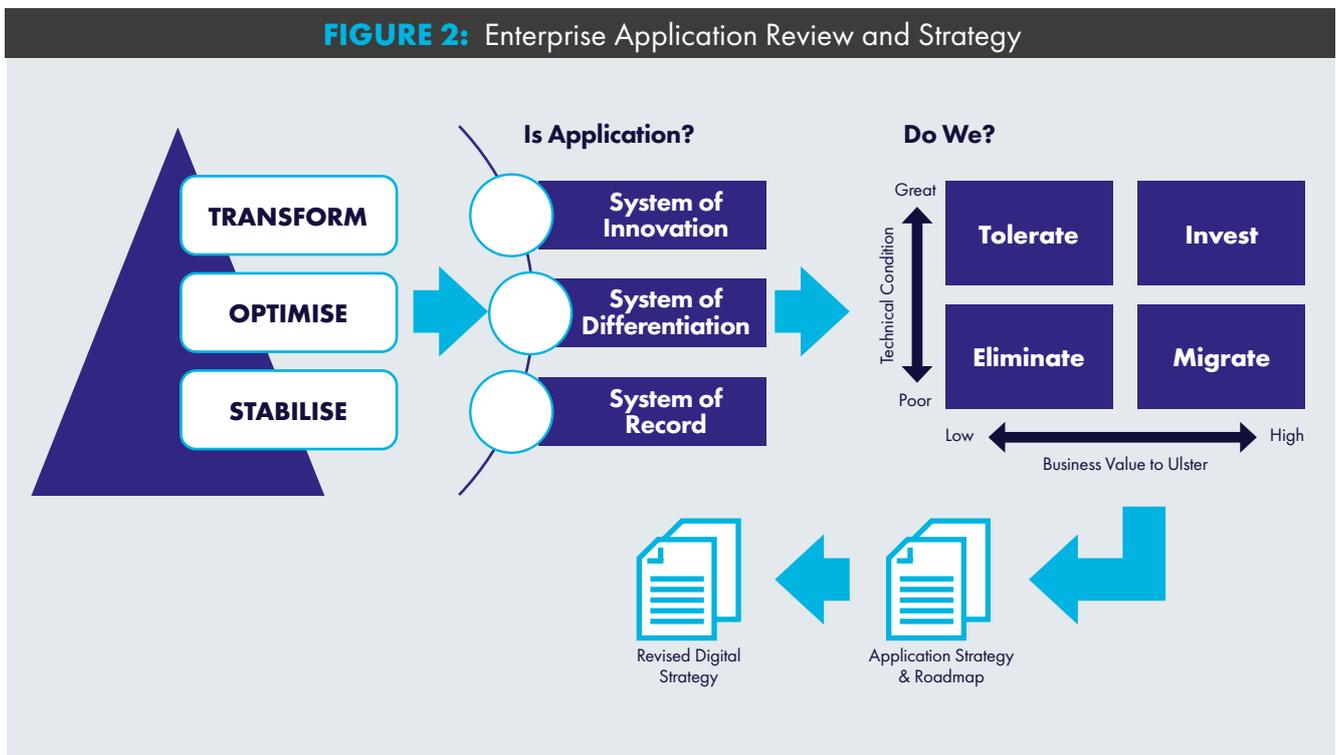


- **Identity and access management**
Control who and what can access your systems and data.
- **Data security**
Protect data where it is vulnerable.
- **Logging and monitoring**
Design your systems to be able to detect and investigate incidents.
- **Incident management**
Plan your response to cyber incidents in advance.
- **Supply chain security**
Collaborate with your suppliers and partners.

ENTERPRISE APPLICATION REVIEW AND STRATEGY

Digital Services will review all applications and through stakeholder consultation identify those that can be tolerated, eliminated, invested in, or migrated, for example to the Cloud or delivered as a Managed Service. Outputs will be used to develop 'optimisation' opportunities and provide input into the development of a longer-term Enterprise Application strategy (Figure 2).

FIGURE 2: Enterprise Application Review and Strategy

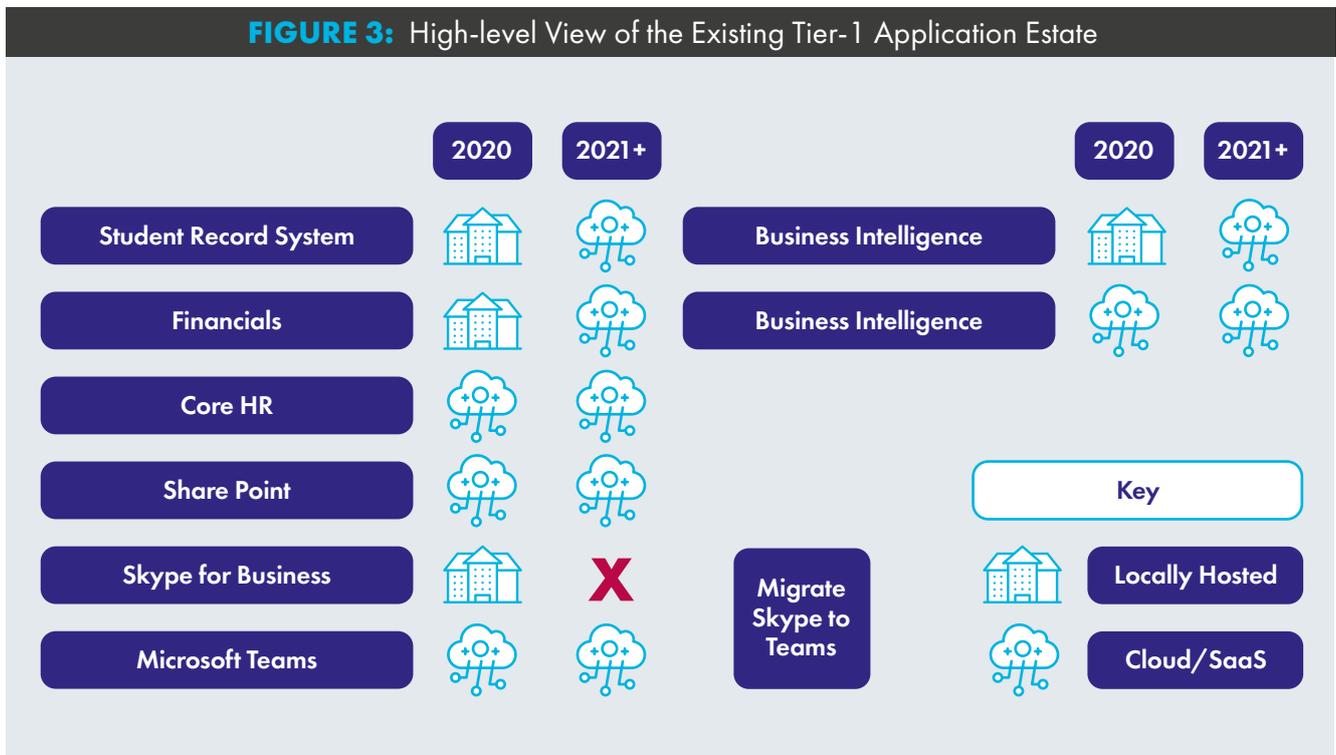


Detailed below (Figure 3) is a high-level view of the existing tier-1 application estate which demonstrates that elements of the 2018 Digital Strategy are progressing, with some applications already migrated into the Cloud and delivered as ‘Software as a Service’, otherwise known as SaaS.

Outliers requiring further assessment include the Student Record System, Financials and Business Intelligence.

Skype for Business is becoming end-of-life and will be migrated across to Microsoft Teams, which is also delivered as a SaaS service.

FIGURE 3: High-level View of the Existing Tier-1 Application Estate



SERVICE MODEL

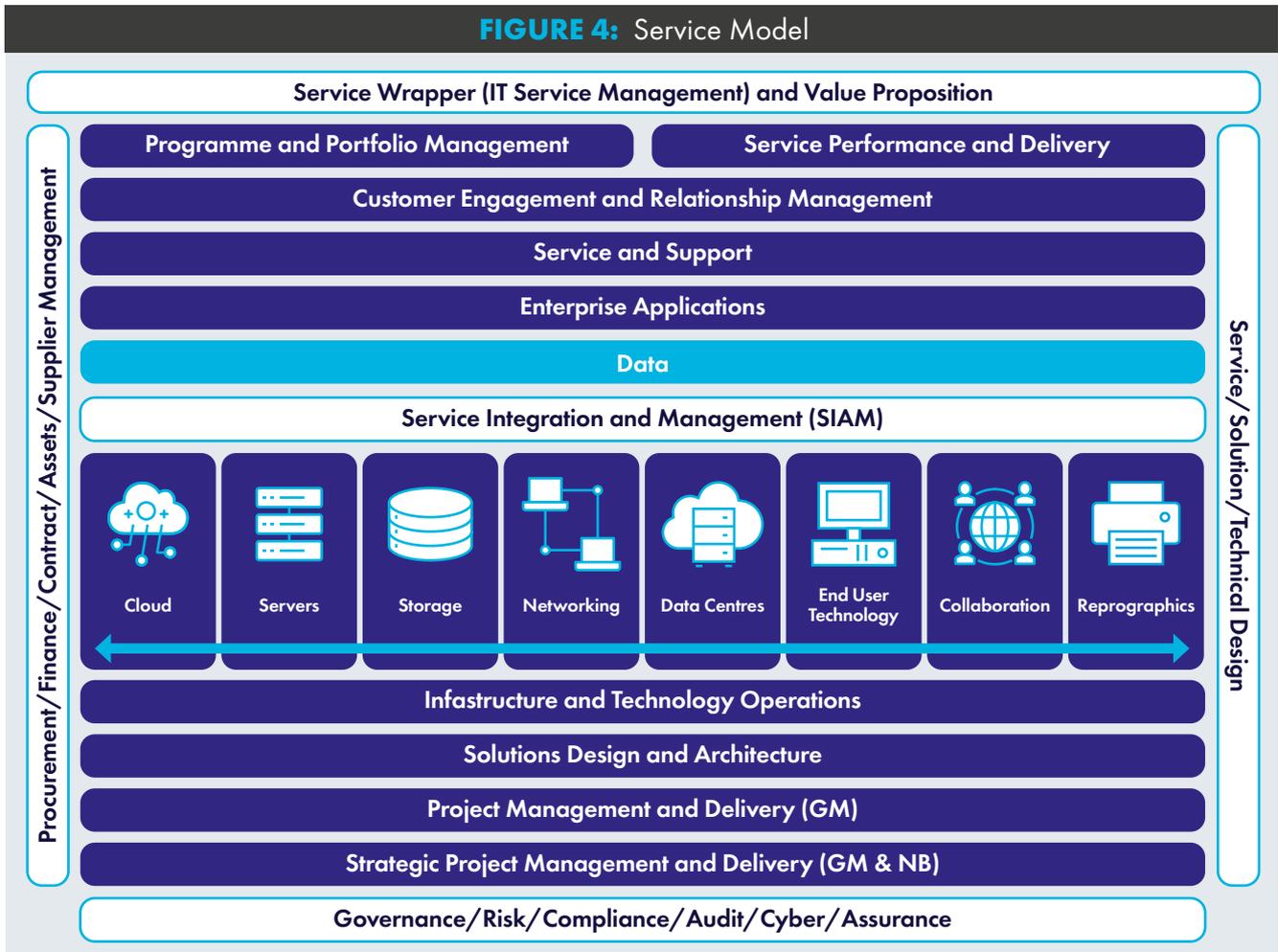
The approach to service modeling is represented below (Figure 4) and based around the SIAM model (Service Integration and Management).

SIAM is recognised as a ‘best practice’ approach to delivery of technology and digital services. In the case of Digital Services this includes a mix of business and digital information technology solutions that integrate into a single business-facing organisation.

SIAM aims to seamlessly integrate services from various sources into a single end-to-end service offer, and in the context of Ulster this includes three elements, namely customers (staff and students), the internal Digital Services function, and external parties such as suppliers and other sectoral partners, for example JISC.

In practice this will ensure improved portfolio management and delivery, enhanced customer experience and access to a dedicated relationship management function.

FIGURE 4: Service Model



Digital Services and our customers will benefit from improved controls around portfolio, demand management and reporting.

Delivery will also require the development of a new set of charters and delivery principles for each function of Digital Services. These will outline the values, the behaviors and approach provided by the newly formed service model.

SERVICE OFFER

Digital Services will operate as a Digital Transformation Partner towards all functions of the University, working in alignment and partnership with staff, students and sectoral partners to develop solutions that are fit for purpose, effective, efficient, and ensure value for money.

We will be instrumental in the standardisation and integration of infrastructure and technology, and with partners will establish new models of service and deliver foundation and transformation services.

SOLUTIONS

These are the key pillars and building blocks of the current solution offer (Figure 5), and Digital Services will further develop and implement formalised Service Level Agreements to improve overall service quality.

FIGURE 5: Current Solution Offer

Infrastructure and Operations	Enterprise Applications	Customer Services and Support	Governance	Digital PMO	GBD Project Delivery	Reprographics
Data Centres	Application Management and Support	Service Desk 1 st Line	Governance	Initiation	Planning	ID Card Production
Servers		2 nd Level Support	Risk Assurance	Planning Requirements	Delivery	Multi-Functional Devices
Storage	Data Management and Integration	Student Support	Cyber	Procurement	Requirement	
Compute		Staff Support	Policy Development and Control	Scheduling	Specification	UU On-Line Copyright Services
Network	Unified Communications	Training	Digital Records Management	Contracts	Procurement	
Cloud	Collaboration	Classroom Support	Information Asset Management	Reporting	Scheduling	Suppliers
Resilience	Database Administration	Teaching Technologies	Software and Hardware Asset Management	Administration	Contracts	National Contracts
Security	Business Intelligence	Audio and Video Conferencing Support	Corporate Licensing and Compliance	Stakeholder Management	Stakeholder Management	
End User Compute	Hosting	Project Workstream Support		Management	ISD Workstream	
Support	Design	Event Support		Workstream Support	Delivery for GBD	
Design	Build			Business Process Change		
Build	Maintain					
Maintain	Administer					
Supplier	Supplier					

Finance – Budget – Workforce – Management – Business Process – Organisational Support

THE PLAN (Stabilise, Optimise and Transform)

2020 to 2021 will represent a period of stabilisation, with 2021 to 2022 focusing on optimisation, and 2022-2023 transformation.

Digital Services will towards this plan whilst maintaining business as usual operations and supporting the delivery of transformation projects. Outlined below are some of the required workstreams.

FIGURE 6: The Plan

STABILISE (2020-2021)	OPTIMISE (2021-2022)	TRANSFORM (2022-2023)
Rebrand ISD – Digital Service	Estate Rationalisation	Real Time and Dynamic Reporting
Service Review and Remodeling	Cloud Strategy	Automation / BOTs / AI / Machine Learning
Application and Information Review and Strategy	Business Intelligence	Full Enablement of Mobile Workforce
New Solution Offer	Performance Reporting	On-demand Service Provisioning
Best Practice (IT Service Management) – Inc. Service Level Agreements (SLAs)	Information Asset Management	Managed Services
*Cyber Security Programme	Web Services	Enterprise Application and Information Strategic Delivery
Communications Strategy	Standardisation and Centralisation	Virtualisation and Cloud Migrations
Extended Service Hours	Security Operations Centre	Integration Services
Monitoring and Tooling	Network Operations Centre	Mobile Apps
Technical Debt (Legacy and Refresh and Replace)	Enterprise Application Strategic Development	
Digital PMO		
Standardisation		

*Note: Additional funding is anticipated in the areas of Cyber Security and tooling.

CONCLUSION

This Digital Strategy is ambitious and represents the beginning of a transformational journey in challenging times, and requires the development and agreement of associated strategies, roadmaps, plans, business cases and projects.

These will be formulated as outputs from the reviews and assessments outlined above.

The direction of travel for the first year will be to focus on stabilisation, moreover the:

- Rebranding and re-modelling of ISD.
- Development of a new vision for digital.
- Completion of 2019 ISD restructure.
- Development and priority implementation of Cyber Strategy and plans.
- Building the case and seeking agreement on and benefits available from the centralisation and standardisation of Information Technology procurement.
- Production and agreement of long-term Enterprise Application strategy, incorporating elements of Business Intelligence, Management Information, Integration, and possibly Data Warehousing.
- Introduction of formalised service approach to delivery based upon best practice, and formalised approach to 'continual service improvement'.
- Delivery against existing commitments.

This Digital Strategy aims to incrementally improve service whilst at the same time remodeling the ISD function to become Digital Services, whilst developing and seeking agreement on future strategies, and moving towards the centralisation and standardisation of the digital and technical estate, whilst delivering overall improvements in service quality for staff and students.

Mark Taglietti

Chief Digital Information Officer

June 2021