WESTERN POWER DISTRIBUTION
Serving the Midlands, South West and Wales

IT Strategy

Author: Mike Keay

Version: 1.1

Date: 01/12/2021

Contents

Strategy Overview 3

Key Drivers influencing the IT Strategy 3

Vision 4

The IR Department 5

IR Key Principles 6

IR Key Principles by IT Function 8

- IT Management 8
- Application Development and Support 9
- Desktop Computing 9
- Server and Database Hosting 10
- Voice and Data Networks 11
- Cyber Security 11

Future Direction 12

- Cloud Computing and Legacy Modernisation 12

Strategy Overview

The IT strategy provides a blueprint for how IT will support and shape WPD's overall business strategy for the remainder of RIIO-ED1 and into RIIO-ED2 and will assist with communicating IT values, methodologies and capabilities to the business stakeholders and end users.

The strategy specifically takes into consideration current and future business and end user requirements for IT services and will look at:

- **High level overview of the current IT department, its core principles, objectives and approaches to delivery of IT services.**
- **The internal and external influences that are shaping the IT strategy.**
- **An outline of the identified and expected future IT projects, services needs of the business and possible technology changes.**

(Please note that although Cyber Security is cited in this document, it is subject to its own more detailed Cyber Security Strategy)

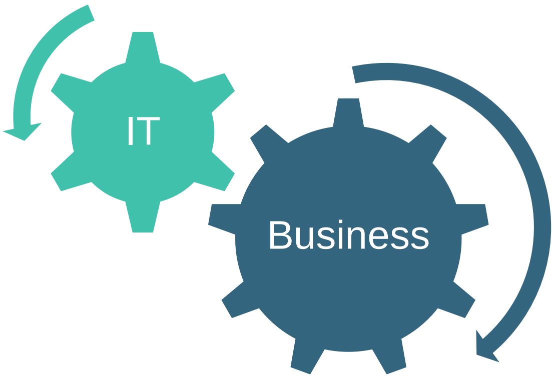

Figure 1 - IT and Business Collaboration

Key Drivers influencing the IT Strategy

The adaption of electricity networks to changes in the way that electricity is generated and consumed has resulted in WPD creating a new Distribution System Operator (DSO) business function to run in collaboration with the Distribution Network operation (DNO) business. The IT department now needs to support both business functions and their differing requirements and expectations for IT.

The DSO business has identified a requirement for a number of new data centric IT projects and systems in RIIO-ED2, which will include providing customer access to our systems and data. To be able to meet these requirements a number of existing legacy applications/systems will need to be modernised to enable better system integration, scalability and data sharing capabilities.

In order to accommodate these identified requirements business and IT strategies need to become increasingly more aligned. Specific business strategies impacting/influencing the IT strategy include:

1. Digitalisation strategy - digitalisation is at the heart of WPD’s transition to building a smart and efficient energy system and underpins our RIIO-ED2 strategy. Digitalisation is the process of using digital technologies to fundamentally change how the network is operating. Over the course of RIIO-ED1 WPD has gradually been increasing the amount of digital technologies on the network – from automation to monitoring equipment.

2. Net Zero strategy - WPD are committed to delivering a network which meets future energy requirements, enabling the transition to a smart, flexible and low carbon energy system in support of the UK Government’s commitment to achieving net zero by 2050.

3. Sensors and monitoring strategy – critical to the successful operation of new DSO systems and processes is good quality, reliable and timely data relating to the state of the network. By the end of RIIO-ED2 WPD are aiming for 100% visibility of its 11kV and higher voltage networks by ensuring that directional power flow measurements are available at all of its Primary substations.

4. Innovation strategy – updated on an annual basis the strategy is focused on the long term development of distribution assets, network operations and customer service in response to changing system and customer needs.

5. Smart Meter strategy – the installation of smart meters will allow WPD to gain much greater visibility of the operational state of the Low Voltage (LV) network and as a result will enhance core business activities, including fault management, network planning and asset management. To ensure the data from smart meters can be used effectively, additional IT systems will be developed.

As well aligning to the afore mentioned strategies, the IT strategy has also taken Government and Regulatory requirements into consideration, with particular emphasis being placed upon the required standards of the General Data Protection Regulation (GDPR), Network Information Systems (NIS) directive and the Technology Security Requirements (TSR).

Vision

The IT strategy has been developed in collaboration with various business units and is aligned to business strategies and regulatory requirements and aims to ensure fit for purpose IT systems are provided to both the DNO and DSO.

It has been identified that there is a need for some IT modernisation in order to address the challenges posed by RIIO-ED2, the DSO and Cyber security. To aid the modernisation transition a short and longer term vision for IT services in WPD has been defined.

Short Term Vision (By the end of RIIO-ED1)

- WPD will adopt a 2 speed IT architecture/culture, with the DSO embracing a more fast-paced cloud-based approach to system/service delivery which embraces innovation. This will require WPD to undertake a number of cloud readiness projects.

- DNO core IT systems (mapping, finance, PowerOn, CROWN) will adapted to enable greater system integration, data exchange and accessibility.

- IT processes, services and staff structures will be changed accordingly in order to accommodate modernisation.

- Common enterprise architecture standards will be defined and implemented across all applications (IT and business supported) and infrastructure to simplify support and maintenance schedules.

- Plans for the modernisation of legacy systems and old technologies will be defined.

Long Term Vision (RIIO-ED2 and into RIIO-ED3)

- WPD will adopt a hybrid cloud architecture, comprising of public, private and on premise environments/solutions providing common services to both the DSO and DNO.

- Legacy systems and old technologies will be either replaced or modernised.

- The development of a common data platform to allow data to be integrated from multiple sources and easily viewed and shared.

- Staff will be better enabled to work from any location and have easier access to the applications, systems and data they require to carry out their jobs.

The IR Department

The core function of the IT department is to support and enhance the delivery of business work programmes by providing highly secure, cost effective, reliable and resilient systems that are aligned with business goals and the delivery of stakeholder commitments and customer expectations.

IT services and systems have to date been aligned to support the activities of a Distribution Network Operator (DNO), responsible for operating, maintaining and repairing the electricity network, providing a safe and reliable electricity service to 8 million customers.

IT services within WPD are currently provided by various in-house teams. Application support for finance systems, mapping and the PowerOn Control systems are provided by business specific teams. All other application, server infrastructure and Local Area Network (LAN) support is provided by the IT department.

The IT department is structured into the following 6 service areas and provides the majority of IT services and support functions to the business through robust and well established business processes and systems and experienced knowledgeable staff:

- IT Management
- Application Development and Support
- Desktop Computing
- Server and Database Hosting
- Voice and Data Networks
- Cyber Security

The function of the IT department is to provide the following high level activities for both new and existing systems:

1. System Design/Architecture
2. System Development
3. System Installation/Implementation
4. System Maintenance
5. System Support
6. System Security

IR Key Principles

The ongoing strategy for delivering IT systems into RIIO-ED2 and beyond is underpinned by five key IT principles:

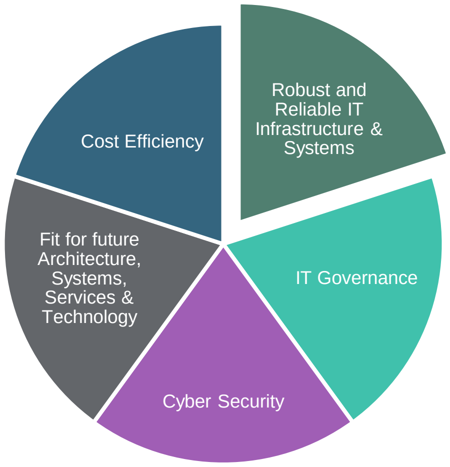

Figure 2 – Key Principles

1. Robust and Reliable IT infrastructure and systems
   a. Suitable levels of resilience will be applied based upon business criticality of the system.
   b. Monitoring, back-up and disaster recovery capabilities will be applied as a minimum to all critical systems.
   c. Hardware, operating systems and software kept in the supported word where possible.
2. IT Governance
   a. Adherence to Information Technology Infrastructure Library (ITIL) best practices where applicable.
   b. Well defined and maintained policies and standards.
   c. Defined responsibilities and ownership.
   d. Executive level accountability.
   e. Imbedded change controls.
3. Cyber Security
   a. Security controls implemented based upon business criticality and risk rating.
   b. Segregation of systems and network to reduce the impact of an intrusion.
   c. Compliance with NIS and TSR regulations.
   d. IT and OT standard cyber security practices.
4. Fit for future Architecture, Systems, Services and Technology

    a. Systems architected and engineered to enable future modification, expansion or change.

    b. An architecture ‘standards based’ approach (common design, implementation, platforms, technologies etc.) to make systems easier to support, integrate and more interoperable.

    c. Continual monitoring of changes in technology and the regular review of systems and processes to ensure they remain fit for purpose.

    d. Regular review and evaluation of services with the business stakeholder.

5. Cost Efficiency

    a. Working closely with WPD’s Procurement team to ensure that any new IT systems or services are correctly and cost effectively sourced.

    b. Challenging our suppliers when renewing contracts to ensure we are always get best price.

    c. Considering total cost of ownership when purchasing any new system or service.

    d. Well defined and cost justified projects.

    e. Only migrating/upgrading existing services to the new technologies where it is cost effective and beneficial to do so, subject to Cyber Security requirements and business drivers.

IR Key Principles by IT Function

IT Management

- Own the corporate IT Computer and Communications policy which outlines the minimum IT security standards that are required to be observed by all WPD IT users.

- Set the overall direction for the IT department, to specifically include vision delivery, budgets, goals and targets.

- Provide overall governance for IT systems and services within WPD.

- Ensure that IT projects are prioritized by business importance and are subject to change controls. Visibility into demand, resources and the project portfolio will made available to share with key business stakeholders.

- Maintain highly skilled internal resource pools.

- Define the frameworks and methodologies by which the IT department operates.

- Align IT services with core business needs and develop and maintain application roadmaps.

Application Development and Support

- A hybrid model of In-house and 3rd Party applications will continue to be adopted with the implementation of in-house systems only being considered when off the shelf or software as a service solutions are not available to meet business needs or where WPD can gain significant business advantage by building a bespoke system.
- 3rd party applications software including PowerOn, Mapping and Finance systems will be administered directly by business units.
- Application development and support teams will be appropriately aligned to specific business functions and their corresponding work programmes.
- The most appropriate development platforms and programming toolsets will be selected on a case-by-case basis depending on cost, technical fit and functional benefits.
- IT disaster recovery and business continuity procedures and their underlying associated technologies will continue to be developed and tested.
- The applications team will work closely with the relevant business teams to develop and maintain a system and data catalogue.
- OWASP standards, procedures and methodologies of secure application development will be adhered to where possible.

Desktop Computing

- A central 1st line support service desk function will manage IT incidents and how IT service requests are fulfilled through the encouraged use of Self Help tools and knowledge base articles.
- Service Level Agreements (SLA's) will be defined and monitored for all service request types, with any service level failures investigated.
- Service levels and support desk performance will be reviewed regularly with business system owners.
- Reporting dashboards will be further developed and key performance indicators established for asset management and service desk tickets.
- The development and use of internal and external messaging and collaboration platforms will be further exploited.

- Desktop computing asset lifecycle will be extended through the use of extended warranties and break fix contracts where appropriate.

- IT assets such as desktop PC’s, Laptops and mobile phones will be managed and monitored throughout their lifecycle.

- Software licensing will be closely managed with unused licenses being removed from users and reissued where possible to ensure the most efficient use of software.

- Access to corporate resources such as SharePoint sites will be expanded to mobile platforms/devices.

- Access to the internet will be provided to desktop computer users through the use of secure services such as virtual desktop internet (VDI).

- Technologies and services will be adapted to better support the adoption of homeworking within WPD, including the reduction in the number of desktop PC’s through the use of virtual desktop solutions and laptop docking stations.

Server and Database Hosting

- Systems will be hosted on virtualized platforms, with dedicated hardware only being utilised where dictated by geographic or application specific requirements.

- Server and database hoisting services will be provided in-house where it is cost effective and beneficial to do so. Outsourcing or the use of contract resource may also be considered when demand out strips supply.

- Operating system patching including security patching will be applied to all systems in a timely manner.

- Hardware and operating system will be kept in the supported world where possible or will be subject to risk mitigation or acceptance and recorded on the risk register.

- New technologies, platforms or service will only be adopted and implemented when required and/or appropriate to do so, e.g. systems can no longer be hosted by WPD.

- WPD’s critical systems will not be subject to outsourcing, cloud or otherwise, unless absolutely necessary.

- The IT department will work closely with the business to identify and test emergent technologies, such as machine learning and artificial intelligence.

- Tier 1 vendors will be utilised where appropriate, with vendors being subject to stringent cyber security standards and controls.

Voice and Data Networks

- Wide Area Network (WAN) circuit carrier diversity (i.e. two different suppliers) at all primary and secondary sites is required in order to provide service resilience.

- Bandwidth will be increased across both local and wide area networks enabling high speed data transfers when available or the demand dictates.

- Wi-Fi will be considered as alternate to Ethernet fixed cabling in providing network connectivity within WPD’s offices.

- The possible future replacement of voice systems dedicated hardware and lines with Session Initiation Protocol (SIP) will be investigated with an emphasis on reliability and availability to maintain a high level of service to WPD.

- Working closely with vendors we will continue to improve unified communications technologies/services (contact centre, mobiles, landlines, etc.).

- Data Centres and Comms rooms will be maintained in-house supported by specialist 3rd party service providers.

- Softphone will be used as a replacement for physical desk phones where appropriate.

Cyber Security

- Cyber security standards and practices will be based on the principles as defined in the NIS directive and will be continually assessed and appropriate counter measures implemented as required.

- All new IT systems will be subject to a security review and risk rating before implementation. All existing systems will be subject to ongoing security assessments with appropriate levels of monitoring, logging and investment then applied accordingly.

- Third party experts will be engaged to provide Security Operation Centre intelligence that WPD will act upon to mitigate vulnerabilities.

- The basic fundamentals of good security practices such as access management, data encryption, Anti-Virus controls, patch management and penetration testing will continue to be placed as high priority with oversight to ensure practices remain appropriate.

- IT will engage with all areas of WPDs business to provide awareness and training on security matters.

- Security policies will detail the standards and controls to be applied to IT services, such as encryption, patching logging and monitoring.

- IT systems will be risk accessed using IR's risk model which rates risk based upon a standard set of Cyber Security benchmarks and business systems criticality before applying any appropriate cyber security controls.

- All IT systems and server network will be disconnected from the internet unless the relevant security controls are in place and agreed by the IRMT. Connected Cloud and BYOD remains strictly prohibited.

Future Direction

Cloud Computing and Legacy Modernisation

In order for IR to be able to meet the future IT aspirations of the business, WPD will need to modernise many of its current legacy systems as well as embrace Cloud technologies and the potential benefits they can offer before the start of RIIO-ED2. The reduction in vendor 'on premise' products/solutions is also driving this requirement.

A number of cloud readiness projects and initiatives will therefore take place during the remainder of the RIIO-ED1 period in order to enable WPD to gain a better insight and understanding of the different types of could technologies, their security limitations and to also determine their suitability. It is then envisaged that a Hybrid Cloud model will ultimately be adopted in RIIO- ED2.

The following cloud pre-requisites have been identified and will be investigated and addressed as part of the planned Cloud readiness projects.

- Development of Cloud security standards, policies and a data classification framework to outlining security requirements for differing WPD data stored in the cloud.

- Identification of suitable Cloud hosting and development, providers, platforms and tools.

- Risk management and categorization of potential cloud providers.

- Staff training on the use of cloud technologies.

- Development of a secure gateway/API platform for enabling Cloud integration to back end IT systems.

- Secure methods of accessing the Cloud from WPDs desktop computers.

- Consideration to the adoption of microservices, web technologies and containerized systems.

Western Power Distribution (East Midlands) plc, No2366923
Western Power Distribution (West Midlands) plc, No3600574
Western Power Distribution (South West) plc, No2366894

Western Power Distribution (South Wales) plc, No2366985
Registered in England and Wales
Registered Office: Avonbank, Feeder Road, Bristol BS2 0TB

wpdnetworkstrategy@westernpower.co.uk