



Arolygiaeth El Mawrhydi dros Addysg a Hyfforddiant yng Nghymru  
Her Majesty's Inspectorate for Education and Training In Wales

17 May 2019

Dear

I am writing in response to your request under the Freedom of Information Act (FOIA) to be provided with information on the series of questions listed in your email below.

Under FOIA, Estyn is required to:

- (i) confirm or deny whether it holds the information of the description specified in the request
- (ii) communicate the information requested to the applicant

In response to your queries, I can confirm the following:

1. ICT/IM&T/IS Strategy- The IT department strategy or plans, highlights their current and future objectives. **This document is attached for your information.**
2. ICT Org Chart- A visual document that present the structure of the IT department, please include name and job titles. If this can't be sent please work towards a structure with job titles. **I attach a copy of the corporate services team structure, which includes IT**
3. ICT Annual or Business Plan- Similar to the ICT strategy but is more annually focused. **This information is included within the ICT strategy attached**
4. ICT Capital Programme/budget- A document that shows financials budget on current and future projects. **I can confirm that the ICT capital budget is £108k**

I hope that this information is helpful to you.

If you are not satisfied with the response Estyn has made regarding your request for information, you are entitled to request that we review the matter. Your request for a review should be addressed to the Feedback and Complaints Manager, and receive no later than 20 working days after the date of this communication.

If you are still not satisfied, you also have a right to complain to the Information Commissioner, who can be contacted at:

Information Commissioner's Office  
Wycliffe House, Water Lane  
Wilmslow  
Cheshire  
SK9 5AF  
Tel: 01625 545 745  
Fax: 01624 524510  
Email: [enquiries@ico.gsi.gov.uk](mailto:enquiries@ico.gsi.gov.uk)

Yours sincerely

**Robert Gairey**

Swyddog Arweiniol Cyhoeddiadau / Lead Officer: Publications

**Estyn**

**Arolygiaeth Ei Mawrhydi Dros Addysg A Hyfforddiant yng Nghymru  
Her Majesty's Inspectorate For Education and Training in Wales**

**Cyfeiriad:** Llys Angor, Heol Keen, Caerdydd, CF24 5JW

**Address:** Anchor Court, Keen Road, Cardiff, CF24 5JW

**Ffôn Estyn/Estyn Phone:** 02920 446309

**E-bost/E-mail:** [robert.gairey@estyn.gov.wales](mailto:robert.gairey@estyn.gov.wales)

**Gwefan/Website:** [www.estyn.llyw.cymru](http://www.estyn.llyw.cymru) / [www.estyn.gov.wales](http://www.estyn.gov.wales)

Mae Estyn yn croesawu gohebiaeth yn Gymraeg a Saesneg. Bydd gohebiaeth a dderbynnir yn y naill iaith neu'r llall yn cael yr un flaenoriaeth.

Estyn welcomes correspondence in both English and Welsh. Correspondence received in either language will be given equal priority.



Dilynwch [@EstynAEM](https://twitter.com/EstynAEM) / Follow [@EstynHMI](https://twitter.com/EstynHMI)

**From:**

**Sent:** 18 April 2019 16:47

**Subject:** Request for Freedom of Information- Information Tech Documents

Hi,

I wish to submit a request for some of the organisation's information around the internal plans and strategy documents around ICT.

The ICT documents I require is the 2019 – Onwards. If any of the documents is for example 2017-2020 please make sure that this is the 2019 version of the document. Or the most recent update.

I wish to obtain the following documents:

1. ICT/IM&T/IS Strategy- The IT department strategy or plans, highlights their current and future objectives.
2. ICT Org Chart- A visual document that present the structure of the IT department, please include name and job titles. If this can't be sent please work towards a structure with job titles.
3. ICT Annual or Business Plan- Similar to the ICT strategy but is more annually focused.
4. ICT Capital Programme/budget- A document that shows financials budget on current and future projects.

If some of these documents are not valid, please state when the 2019 ICT documents are planned to be published.

Please do get back to me if you have further questions or feedback.

Thanks in Advance



## ICT Strategy v0.1 DRAFT

## Version Control

Version	Date	Contributor	Approval
0.1	26/04/2019		For Information Systems/Governance Group (May 2019 meeting)

## Table of Contents

1	Foreword.....	6
2	Executive Summary.....	6
3	Organizational overview .....	8
3.1	Strategic Priorities.....	8
3.1.1	Donaldson Review.....	8
3.2	Challenges .....	9
3.2.1	Capital and Revenue Funding .....	9
3.2.2	Staff Developmental Changes.....	9
3.2.3	Changes in Working Practices.....	9
3.2.4	Increased Cyber Threat .....	9
3.3	Additional Drivers .....	10
3.3.1	Software Licensing Marketplace .....	10
3.3.2	Infrastructure and Software Refresh .....	10
3.3.3	Prevalence of Cloud Technologies .....	10
3.4	Benefits of the Cloud .....	10
3.4.1	Scalability .....	10
3.4.2	Capacity Management .....	10
3.4.3	Resilience .....	11
3.4.4	Security .....	11
3.4.5	Maintenance .....	11
4	Current ICT situation.....	12
4.1	Current Architecture .....	12
4.2	User Types and Equipment provided.....	13
4.3	Corporate Applications .....	13
5	ICT Strategy.....	14
5.1	Strategic Principles.....	14
5.2	Target Operating Model.....	15
5.3	Technical Initiatives.....	16
5.4	5 Year timeline .....	17
5.4.1	Cloud Build Out .....	17
5.4.2	Extend AD to Azure AD .....	18
5.4.3	Zscaler Implementation .....	18
5.4.4	SharePoint Migration .....	18

5.4.5	Device Replacement .....	18
5.4.6	Cloud PBX.....	19
5.4.7	Intune Device Management.....	19
5.4.8	Conditional Access .....	19
5.4.9	Cyber Reporting .....	19
5.4.10	AAD Authorisation and Authentication .....	20
5.4.11	Migrate to Skype Online or Teams.....	20
5.4.12	Migrate Mailboxes to Exchange Online .....	20
5.4.13	Cloud Backup.....	20
5.4.14	SQL Re-platforming .....	20
5.4.15	Data Reporting .....	21
5.5	Additional Items.....	21
5.5.1	Operating System Strategy .....	21
5.5.2	Datacentre Strategy .....	21
5.6	Disaster Recovery.....	21
5.7	Business Continuity.....	21
5.8	Application Strategy.....	21
5.9	Supplier Strategy.....	22
5.10	Telephony .....	22
5.11	Print.....	22
5.12	Retention and Disposal .....	22
5.13	Assisted Users .....	22
5.14	Support.....	23
6	Governance.....	24
6.1	Information Strategy Group.....	24
6.2	Information Services Team .....	24
7	Annex A – Cloud Options Analysis .....	25
7.1	Types of Cloud Service .....	25
7.2	Marketplace Analysis .....	26
7.2.1	Comparison of Cloud Services.....	26
7.2.2	Comparison Methodology .....	26
7.2.3	Compatibility (with current and future estate) .....	27
7.2.4	Flexibility .....	27
7.2.5	Ease of migration .....	27
7.2.6	Resilience .....	28
7.2.7	Security .....	28

7.2.8	Cost .....	29
7.2.9	Summary .....	29
7.3	Option Analysis .....	30
7.3.1	Option 1 – Do Nothing (stay on premise) .....	30
7.3.2	Option 2 – Move all systems to Azure Cloud capability.....	30
7.3.3	Option 3 – Enable Cloud capability .....	31
7.4	Recommendation.....	31
8	Appendix B – ICT Support Option Analysis .....	32
8.1	Purpose .....	32
8.2	Background .....	32
8.3	Option Analysis .....	33
8.3.1	Option 1 – Do Nothing .....	33
8.3.2	Option 2 – Re-procure Existing Supplier .....	33
8.3.3	Option 3 – Procure a new Support agreement.....	33
8.3.4	Option 4 – Build an in-house ICT Service .....	34
8.3.5	Option 5 – Use a Public Sector Shared Service .....	35
8.4	Recommendation.....	35

## Table of Figures

Figure 1 - Current Architecture overview .....	12
Figure 2 - User Types.....	13
Figure 3 - Strategic Principles.....	14
Figure 4 - Target Operating Model .....	15
Figure 5 - 5 Year Timeline .....	17
Figure 6 - Types of Cloud Service and division of responsibility .....	25



## 1 Foreword

This ICT Strategy has been put together in order to help us take a strategic view of ICT over the next five years. The key premise of an ICT Strategy should be to help an organisation meet its future goals, and to ensure the right tools are available to staff to help them as effectively as possible – with IT as an enabler, not a blocker.

Inevitably, organisations will change over time, therefore it is imperative that an organisations ICT infrastructure and supporting contracts are flexible enough to be able to support that change. In this day and age, applications, infrastructure and systems are the beating heart of any organisation, and we cannot function without them. It is critical therefore, that we are able to defend against growing and industrialised Cyber Threat by protecting and monitoring our infrastructure and safeguarding our data. We must also continue to be vigilant in how we handle information and how we physically protect our assets; most data leaks are still caused by human error. With complexity, comes the risk of equipment failure, so we must also ensure our ICT Systems are able to meet our Disaster Recovery and Business Continuity needs.

In light of Professor Donaldson’s “Learning Inspectorate” review, it is possible that changes to the way we operate will be implemented and we need to ensure our ICT will be able to support us through this process. For example, if it is required that we undertake more inspections, and work with more stakeholders then it is critical that we are able to work anywhere and use the latest tools to ensure we can collaborate more effectively. Being able to work anywhere, also makes us a more resilient organisation, as well as helping staff balance the demands of their home lives with work more easily.

This strategy also sets out how we will gradually adopt cloud technologies, scaling down our physical datacentres over a number of years and ensuring we benefit from having the latest applications on our desktops. This move away from physical servers will also help ensure our infrastructure is future proofed, as well as moving away from costly server replacement cycles and helping us have more predictable costs.

Overall, the details and roadmap detailed herein, describe how we will continue to meet the needs of our organisation over the coming years.

## Executive Summary

To be completed following agreement of roadmap by Information Systems/Governance Group

## 2 Organizational overview

Estyn is the body responsible for inspecting learning settings in Wales, including:

- Non-maintained nursery settings
- Schools
- Work Based Learning locations
- Further Education
- Local government education services
- Initial teacher training

Estyn provides advice to the Welsh Government on quality and standards in education and training in Wales and publicises and promotes good practice based on inspection evidence.

As at April 2019, Estyn has 120 staff, which comprises corporate and management staff based at Anchor Court in Cardiff, and home-based Her Majesty's Inspectors (HMI). Third-party inspectors also undertake inspections for Estyn, as part of inspection teams.

### 2.1 Strategic Priorities

Estyn's Strategic Priorities can be categorized into three main areas

#### 1 Statutory Functions

Estyn is required to undertake its statutory inspection duties on learning settings across Wales

#### 2 Thematic Reviews

Annually, Welsh Government will request particular themes relating to the education system have particular emphasis – for example bullying.

#### 3 Building capacity and support for the education inspection system

Estyn provides training for inspectors and hosts best practice events in order to share knowledge and good practice within the education sector.

#### 2.1.1 Independent review

An independent review of Estyn by Professor Graham Donaldson has recognised the important role that Estyn plays in Wales' developing educational landscape.

Some of the key recommendations of the report are as follows:

- An enhanced role for Estyn in providing evaluation and support at the school, local authority, regional, and national levels.
- Mobilisation of Estyn's resources to kick-start reform with an initial short pause in the inspection cycle to allow inspectors and schools to work together on the reforms.
- Increased responsibility for schools to evaluate their own performance with confirmation of the quality of that self-evaluation by Estyn.
- More informative inspection reports with rounded evaluations replacing summative grades.
- More tailored focus on schools causing concern with diagnostic inspections providing better insights into necessary changes.

- Timely evaluation of progress with reforms nationally through thematic reporting and a three-yearly 'state of the nation' HMCI Report.
- Further entrenching Estyn's independence.
- Need for alignment across the accountability landscape.

These recommendations and the fact that Estyn's role will widen along with the need for more detailed reporting will need to be underpinned by future ICT provision. Therefore, these will be key drivers for Estyn's strategy

## 2.2 Challenges

Estyn have identified a number of challenges going forward:

### 2.2.1 Capital and Revenue Funding

Whilst capital funding levels have been largely maintained, annual real-terms cuts to revenue funding have been experienced by many public sector bodies, including Estyn, during the past decade of austerity. In the era of cloud computing where the consumption of compute power and storage is billed per second and charged on a monthly basis, greater revenue funding and less capital is required. This is becoming recognised by both Central and Welsh Government and it is hoped will translate into changes of the funding model for Estyn.

### 2.2.2 Staff Developmental Changes

As the nature of inspections change as a consequence of the Donaldson review, it is likely that staff may need to expand roles, and this will require ongoing collaborative discussions. It is also important, as people change roles, that the systems which provide core services are easy to use.

### 2.2.3 Changes in Working Practices

Estyn is likely to increase the number of staff working in a mobile fashion going forward. Changes in working practices across many sectors have typically meant greater flexibility for staff whom are normally office based to work from any location (for example home, or a different office). Changes in technology and working culture are now enabling this to become more widespread.

### 2.2.4 Increased Cyber Threat

The frequency and complexity of Cyber Attacks continues to increase, as cyber-attacks become more professional and advanced. It is critical therefore that Estyn protects its systems proportionately. In many Cyber Attacks human vulnerability still plays a critical part, (for example, clicking a link in an email, downloading malicious software, complying with a phishing request), therefore it is vital that Estyn's staff are well informed with regard to how to recognise a cyber-attack and the next steps to take.

## 2.3 Additional Drivers

### 2.3.1 Software Licensing Marketplace

Her Majesty's Government (HMG) have recently signed a new Digital Transformation Agreement (DTA) contract with Microsoft for provision of Microsoft licences for Microsoft Office, Windows, Identity and Device Management services. The new DTA came into effect on 1<sup>st</sup> April 2019 and has adopted a "cloud first" approach that results in services becoming more expensive to operate on-premise than in the Microsoft cloud.

### 2.3.2 Infrastructure and Software Refresh

All hardware has a life span, and there is currently a number of hardware items that are scheduled for refresh this calendar year. It is therefore timely that we examine our options with regard to the hosting of our ICT systems.

### 2.3.3 Prevalence of Cloud Technologies

Many Software manufacturers including Microsoft are now prioritising their cloud offerings over traditional on-premise solutions. This will mean, that organisations which have failed to adopt cloud technologies will be left behind, in terms of the service they can provide staff and their external stakeholders. Central and Welsh Government are both proposing Cloud First approaches and a number of Public Sector organisations have already successfully adopted cloud-based infrastructures and solutions. The wider benefits of Cloud based solutions can be summarized as follows in section 3.4

## 2.4 Benefits of the Cloud

### 2.4.1 Scalability

Cloud services are much easier to scale than traditional on-premise environments. In an on-premise environment, in order to scale an application, we would have had to purchase an additional server or storage, wait for it to arrive (which could be weeks), build it, test it, and then implement it. In the cloud, we can add scale to a system in seconds, and we can support enormous user bases by adding servers to solutions as required. We can also implement a new server in less than five minutes.

### 2.4.2 Capacity Management

For on-premise environments, Capacity Management has meant firstly ensuring that servers and storage were powerful and big enough when purchased and then adding to them if necessary throughout their lifecycle. With cloud services however, there is also the ability to turn servers and storage down, often without interrupting service. This means that if there is less consumption than anticipated when a service is first implemented in the cloud, then the servers and storage associated with the service can be turned down as required. Periodically monitoring server utilisation can produce substantial savings, as well as helping to ensure that the service runs optimally. Furthermore, with Azure, a "Reserved Instance" is available; this basically allows you to purchase upfront a type of server for either one or three years. Doing so allows a cost reduction of up to 50%. Reserved instances can be cancelled and exchanged should needs vary over time and can be applied to any server. As the cloud evolves there are also new products that can be used to simplify architecture and reduce costs, therefore it is a critical that a regular focus on cost optimisation is undertaken.

#### 2.4.3 Resilience

The physical resilience in cloud datacentres is much greater than most organisations can afford independently. Datacentres already have resilient power, cooling, fire suppression, generator facilities and military grade security as standard. Using these shared datacentre facilities by virtue of consuming cloud services, means that our organisation will also become more resilient with the ICT becoming more highly available. All main cloud providers also provide financially backed Service Level Agreements (SLAs) regarding availability.

#### 2.4.4 Security

Cloud perimeter security is again, industrial grade, and typically much greater than an individual organisation could afford to implement and maintain. Security of SaaS offerings is very high, with system patching being undertaken by the vendor (usually on an immediate basis). PaaS services will also have the underlying platform patched, whilst IaaS services usually require the customer to ensure that patching is undertaken – although there are many new cloud-based tools available to make sure that this is a simple process.

#### 2.4.5 Maintenance

Whereas with on-premise systems, all aspects of the infrastructure would require physical maintenance from time to time, using cloud systems vastly reduces that. Indeed, with PaaS, SaaS and IaaS offerings, all physical maintenance is removed, with underlying hardware being provided seamlessly as part of the service. Maintenance regarding patching of operating systems and applications varies between each variety of the cloud, as illustrated in [Figure 6 - Types of Cloud Service and division of responsibility](#).

Patching is also often undertaken by the Vendor. This means that there is substantially less input required from ICT engineering, and often patching is undertaken without interruption to service. Occasionally, if a patch is urgent (i.e. worldwide cyber-attack such as WannaCrypt), the cloud vendor will patch servers and infrastructure devices during the night without recourse to the customer.

An in-depth review of cloud options is included in discussed in

[Annex A – Cloud Options](#) Analysis.

### 3 Current ICT situation

#### 3.1 Current Architecture

Currently Estyn has a traditional on-premise architecture hosted across two separate sites, operated on their behalf by Westgate IT. The purpose of the two sites is to provide a backup in the instance of failure or loss of the primary site. The time to recover from such a failure would depend on its specific nature, however, in the instance of irretrievable loss of the Primary Datacentre, then it is estimated it could take a number of weeks to fully-restore service in the Backup Datacentre, with current configuration.

The servers are predominantly deployed in a virtualised environment using VMWare and user devices are connected to the main network in Anchor Court, either via direct ethernet connection or via Wi-Fi. A mobile access solution is provided via VPN and RSA token.

Conceptually, the current infrastructure is illustrated below:

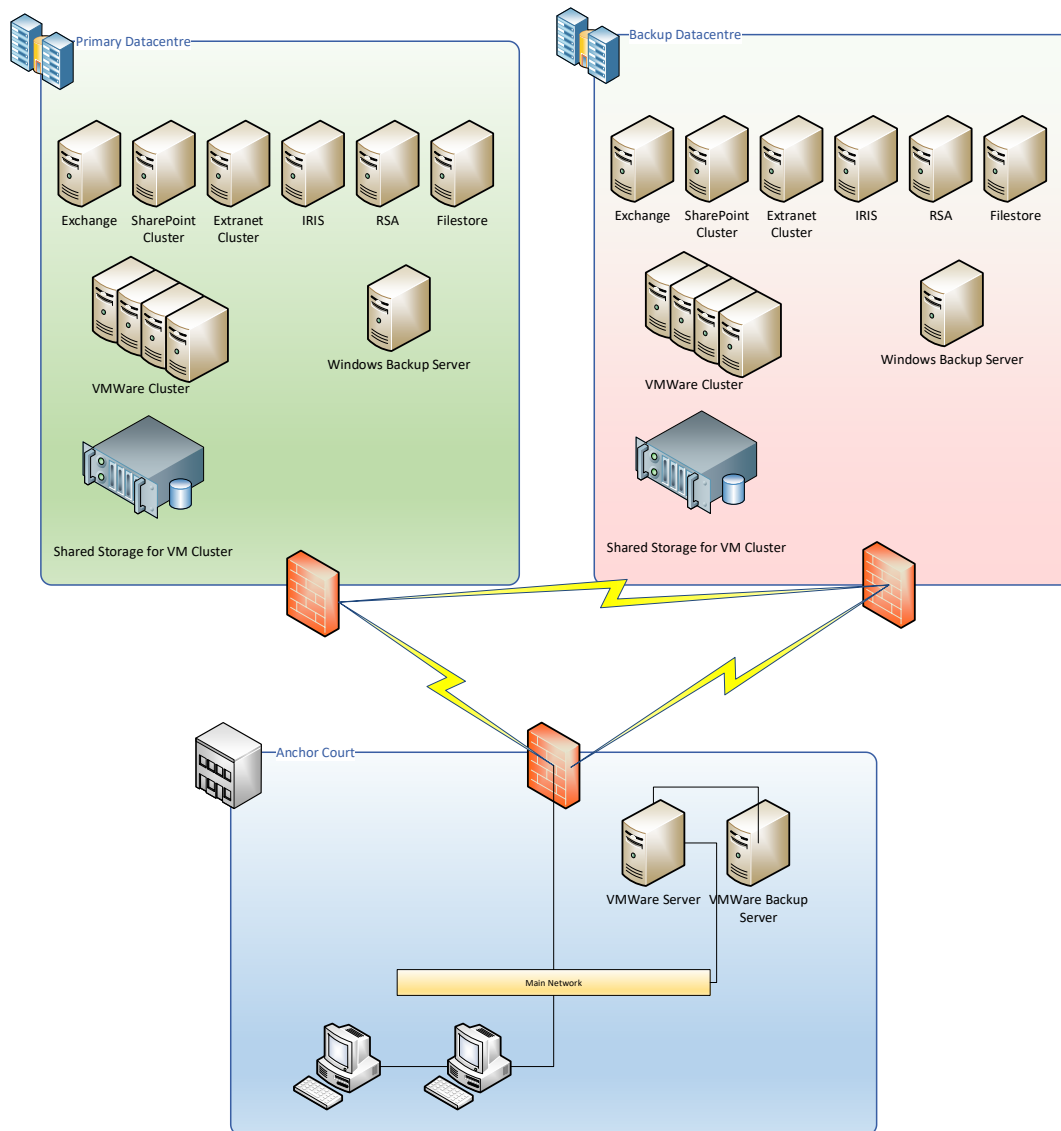


Figure 1 - Current Architecture overview



### 3.2 User Types and Equipment provided

Users of Estyn’s ICT Systems include both internal and external customers. As it stands, users are equipped as per the table below.





				 Website	
Office User	<input checked="" type="checkbox"/>	If Reqd	If Reqd	<input checked="" type="checkbox"/>	Staff based predominantly in the office
Home User		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inspection Staff
Mobile Users		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Internal and External Inspectors and Providers
Stakeholders				<input checked="" type="checkbox"/>	Website visitors

Figure 2 - User Types

As flexible working becomes more widespread, Estyn will begin phasing out traditional desktop machines and will provide laptops to all staff. As well as providing greater flexibility, it will also reduce the complexity of the user estate, making it easier and more cost effective to manage; fewer machine types equates to cheaper maintenance, swifter implementation of patches and better security. Additionally, a wholesale move toward mobile computing is one of the enablers to having cloud-connected devices.

### 3.3 Corporate Applications

The current main Corporate Applications in use by Estyn as follows:

- Microsoft Office 2016 – This is the Standard Productivity suite for staff
- VIR (The Virtual Inspection Room) – an externally facing SharePoint based application providing the ability to undertake inspections and collaborate with inspection teams.
- Cygnum – this is used to schedule work planning for inspectors provided by CACI
- Exchequer – this is finance software provided by Advanced.
- Manage Engine – this is used to manage software rollout and patching levels
- Eventsforce – Event management software
- Deslock – this is encryption software used on staff machines, however, all New laptops have TPM chips, enabling BitLocker to be used in future.
- Tensor – this manages staff leave and time worked

## 4 ICT Strategy

### 4.1 Strategic Principles

The purpose of the ICT Strategic Principles is to provide guidelines for the purchase of new ICT systems and the evaluation of existing systems during periods of review. The principles are the high-level underpinnings of the strategy and reflect the organisation’s future requirements as described in [Organizational overview](#).



Figure 3 - Strategic Principles

## 4.2 Target Operating Model

The Target Operation model illustrated below, describes the end result of the implementation of this strategy; there is a description of the Target Operating model beneath.

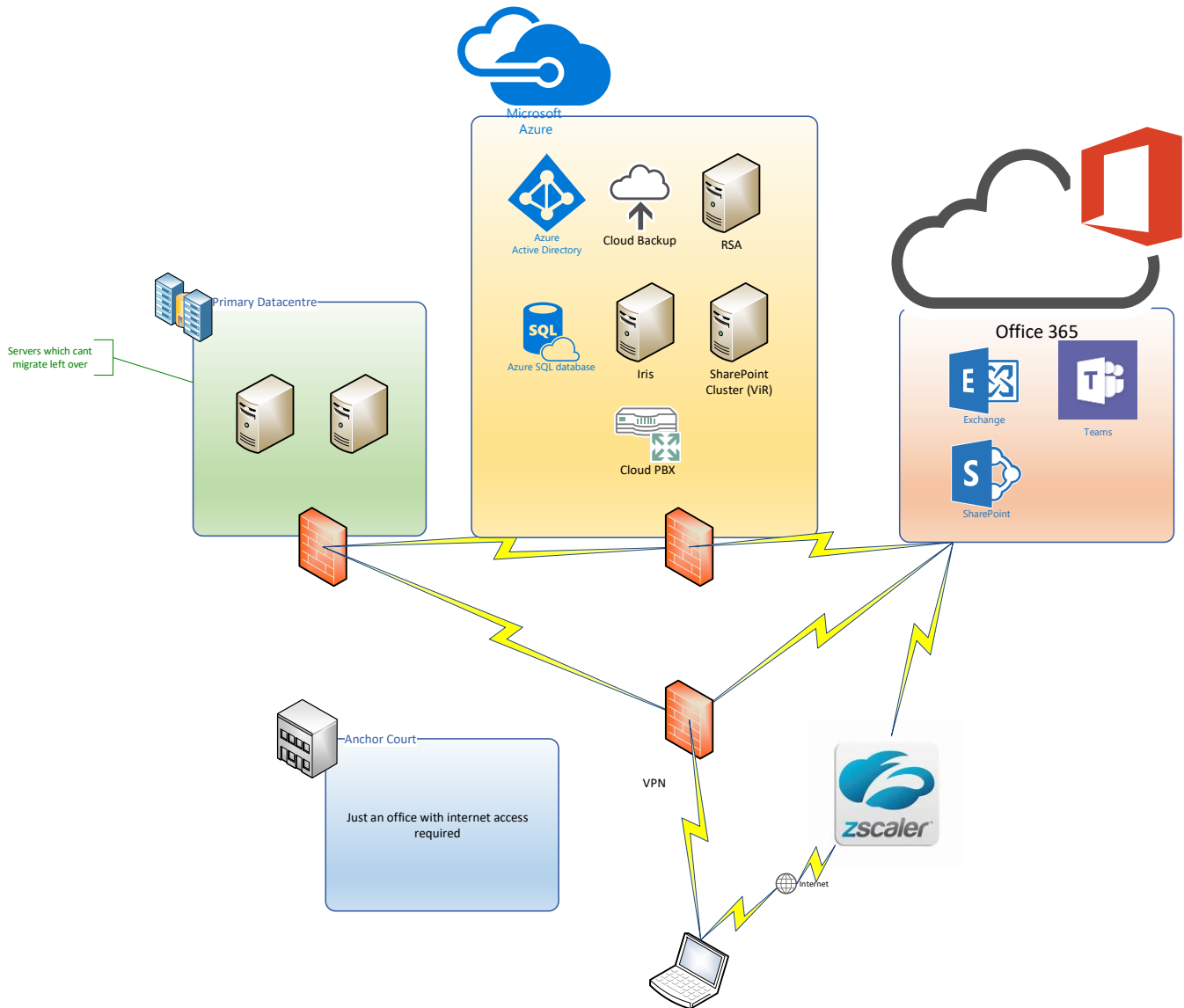


Figure 4 - Target Operating Model

In this model, Estyn have moved to a predominantly cloud-based architecture. As the recommended approach is to utilise already purchased equipment until it is end of life, it is likely that there will be some items remaining in the datacentre. Additionally, some systems are unable to be moved to the cloud, therefore an onsite presence may remain for some time.

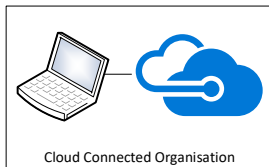
Some of the key features of this model are as follows:

- SharePoint servers are removed, and SharePoint is now provided as part of Office 365
- Exchange servers are removed, and Exchange is now provided as part of Office 365
- Secondary Data Centre decommissioned

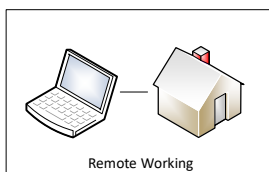
- All users are mobile users, and can connect from any internet connection
- Due to the resilient design, in the event of failure of either the on-premise network or connectivity to Azure services, Users will still be able to undertake core tasks such as emailing and accessing the corporate document repositories
- Ageing SQL databases are moved to Azure
- A cloud PBX has been implemented, meaning that users can access traditional telephony via MS Teams, no matter their location, as long as they have an internet connection
- Structured cabling is no longer required in Anchor Court – only Wi-Fi and an internet connection is required
- Web Filtering is undertaken by Zscaler or similar product, meaning that wherever users connect their laptop, their browsing will be safe
- The in-built defences of the cloud managed services mean greater cyber resilience for Estyn
- The enhanced device management and control brought in by implementing MS Intune also increases the layer of cyber defence we have on each device.
- Physical maintenance of servers is greatly reduced, as servers are deprecated and replaced by cloud services instead

### 4.3 Technical Initiatives

In order to support the organisation's future needs and goals and to implement the Target operating model there are four main tranches of work required through the duration of the strategy, which are described below:



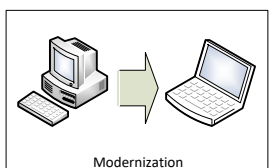
Making the organisation ready to consume cloud services and realising the potential to have cloud-connected devices



Enabling our staff to work anywhere anytime



Making sure we develop our new systems to be able to withstand modern cyber threat.



Making sure we have access to the latest software tools, particularly in the collaboration space

## 4.4 5 Year timeline

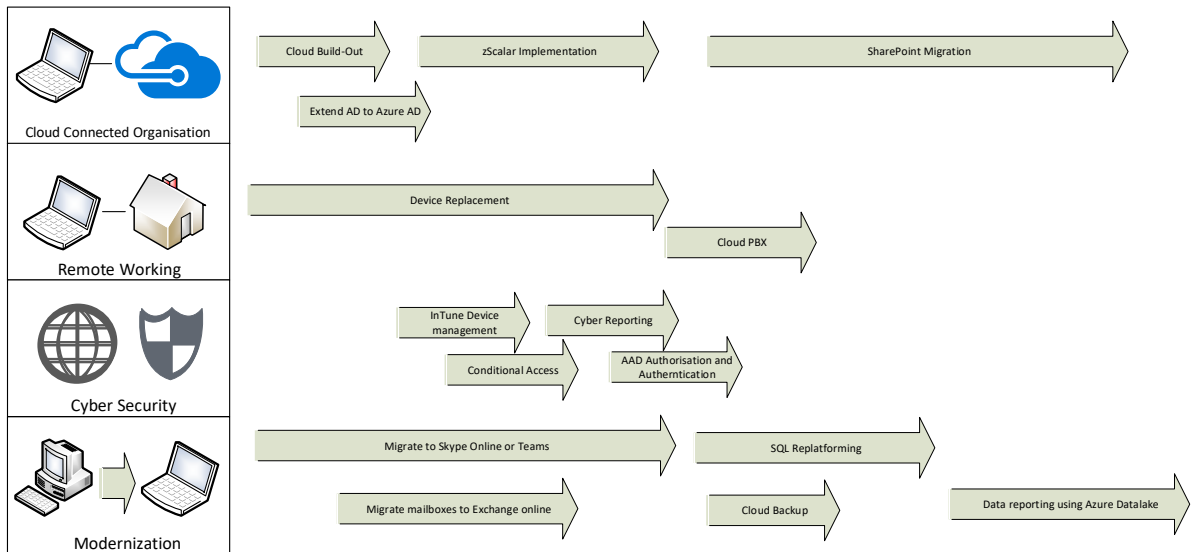
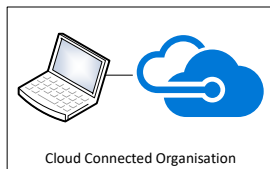


Figure 5 - 5 Year Timeline

**TIMELINE AND ITEMS TO BE AGREED:** by Information Systems/Governance Group

### Build Items



#### 4.4.1 Cloud Build Out

The cloud build-out, which is required to provide Estyn with cloud capability. This capability can then grow or shrink as required. The tasks involved are:

- Network Discovery - Discovery of network infrastructure, including verification of Internet channel, firewall (versions etc), physical port capacity, address space and routing
- Network Design - Design of Azure VNET, associated subnets, NSGs, UDRs, VPN connection, firewall rules on local physical host and virtual appliances
- Create VNET - Create Azure VNET, associated NSGs and UDRs
- Deploy Firewall Virtual Appliances - Create 2 x Virtual Firewall Appliances in Azure and configure for resilience
- Configure VPN - Create IPSec VPN to Azure VNET, including configuration of firewall rules on physical host as required
- Design Azure Subscription - Design of Azure subscription and definition of accounts, departments, Management Group to apply policies and initiatives
- Data Migration Service Design - Includes verification of dependencies such as VMWare version, etc.
- Provision of Log Analytics - Create Log Analytics workspace and automation account

#### 4.4.2 Extend AD to Azure AD

This essentially enables a copy of the on-premise Active Directory to be replicated into Microsoft Azure. Once this is created, authentication can be performed for cloud services from any location over the internet. It also allows Estyn to connect to 3<sup>rd</sup> party cloud services and have single-sign on from the desktop

#### 4.4.3 Zscaler Implementation

This solution proposes the implementation of the Zscaler cloud security service. Zscaler enables secure access to the Internet and Internal services, regardless of the user's location or device. Zscaler provides inline inspection of all traffic to ensure that nothing bad comes in and nothing good leaves.

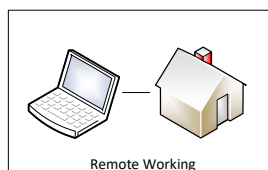
Two Zscaler products will be deployed: Zscaler Internet Access and Zscaler Private Access. ZIA provides secure outbound Internet connectivity providing access control and threat prevention; ZPA provides a zero-trust secure remote access to Estyn applications and services hosted on the Estyn internal network.

Providing Estyn with cloud connected devices provides the following benefits:

- Greater flexibility and mobility for Estyn staff;
- Increased organisational resilience – in the event of a datacentre failure, staff will still be able to access email and the VIR system, their key tool for inspections;
- Increased security for client devices when accessing Internet and on-premise services;
- Internal applications are never exposed to the Internet and users are never connected to the internal network;
- Decommission of legacy client VPN service;
- Decommission of legacy RSA infrastructure;
- Access to modern, secure managed service for Multi-Factor Authentication services; and
- Implementation of infrastructure components to enable a simpler transition to cloud-based services in the future or enables an ongoing hybrid platform as long as is required.

#### 4.4.4 SharePoint Migration

Moving all traditional file stores and SharePoint sites onto (not including VIR) into SharePoint Online as part of Office 365 will remove onsite backup and storage requirements and enable Estyn to more heavily utilise Office 365 licensing.



#### 4.4.5 Device Replacement

Providing new mobile devices to all Estyn Staff will allow them to be able to work from anywhere, anytime, when coupled with the Zscaler and cloud PBX implementation. As well as

providing greater flexible working opportunities for staff, this approach also substantially increases organisation resilience. Some examples are as follows:

- A snow day – users can work from home
- A datacentre outage – users can still connect to SharePoint libraries, email and telephone services
- Family illness/childcare issues/parcel deliveries – users can work from home

#### 4.4.6 Cloud PBX

This allows users to connect to traditional telephone from MS Teams, by having a virtual PBX based in the cloud. Handsets are no longer required (although they are available), and neither are fixed desks. This means that someone takes their landline number with them, wherever they connect their device without needing to worry about logging in or diverting calls.



#### 4.4.7 Intune Device Management

Using MS Intune to manage all Estyn devices will provide the Cyber Security assurance around:

- Ensuring security policies are uniform and implemented on all devices
- Reporting on patching levels
- Implementing patches
- Reporting on unusual activity or locations for devices
- The ability to trace or remotely wipe missing or stolen devices

#### 4.4.8 Conditional Access

These policies are implemented via Intune, and they make sure that devices only meeting certain conditions are able to connect to Estyn's systems. These would likely include:

- Prevention of connection from certain countries (can be over-ridden for planned vacations)
- Prevention of login for impossible travel situations (i.e., a login attempt from Australia, 12 hours after a UK based login)
- Prevention of devices joining that aren't at latest patch or functional levels

Reporting on attempted breach of these conditions is also provided.

#### 4.4.9 Cyber Reporting

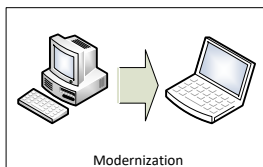
This task involves the implementation of a dashboard that would collate real-time information from all datacentres and services, and also provide real-time alerting. The dashboard is configurable, but could include

- Attempted logins (by location, time, failed, success)

- Quarantined mail items
- Detected mail payloads
- Detected attempts to upload mal-items into SharePoint

#### 4.4.10 AAD Authorisation and Authentication

Azure Active Directory (AAD) is Azure's preferred multi-tenant cloud directory service, capable of authenticating security principals or federating with other identity providers, such as Microsoft's Active Directory. AAD allows application of various kinds (web applications, Windows desktop applications, Universal applications, mobile applications, etc.) to uniformly authenticate. This allows Estyn's users to authenticate via the cloud from any location. It also lets Estyn use 3rd party cloud services and integrate authentication with them, via single sign-on, meaning a seamless users experience.



#### 4.4.11 Migrate to Skype Online or Teams

Moving current Lync servers to Skype Online or Teams will allow Estyn to remove datacentre infrastructure, lowering maintenance and take advantage of the latest functional aspects of MS Teams.

#### 4.4.12 Migrate Mailboxes to Exchange Online

Migrating mailboxes into Office 365 allows Estyn to decommission more datacentre infrastructure. It also means that the service will be looked after by Microsoft, so no server maintenance is required. Additionally, storage is also part of the service, so on-premise mailbox storage can also be decommissioned.

#### 4.4.13 Cloud Backup

Moving backup services to the cloud allows the removal of onsite backup and also reduces the need for a secondary on-premise data centre. Cloud backup can be fully automated, and reports can be built into the overall service dashboard. If required, Geographical resilience can be used to automatically copy backups to two different locations.

#### 4.4.14 SQL Re-platforming

Estyn's SQL platform is ageing and would benefit from being upgraded. Moving Estyn's SQL databases to either SQL Azure or Azure Datalake will substantially increase performance and also enable much better Data Reporting.



#### 4.4.15 Data Reporting

Introducing Power BI and Azure data lake will allow Estyn to produce graphical reports to allow easy analysis of data held regarding inspections and inspection outcomes. This will be particularly relevant as a consequence of the Donaldson Review, to allow the review of consequent changes in ways of working.

### 4.5 Additional Items

#### 4.5.1 Operating System Strategy

Estyn will operate Windows 10 on all devices, which will be remotely managed by Intune and SCCM.

#### 4.5.2 Datacentre Strategy

Once we have enabled cloud capability, we will prioritise the decommissioning of the secondary data centre in order to save costs. This will mean that backup services will either be moved to the cloud or will be built into SaaS and PaaS offerings. For example, the backup integrated into SharePoint.

### 4.6 Disaster Recovery

Currently, in terms of DR – current arrangements are half a day restore, and it is considered that Estyn can tolerate the loss of half a day's data and half a day's work.

Disaster Recovery testing has been undertaken on some applications, however it has not been undertaken for a full data centre outage.

Individual Systems Owners are responsible for the Disaster Recovery of their applications within Estyn and a formal schedule for testing exists.

Whilst enabling cloud capability brings much greater resilience to Estyn, it is recommended that a full Disaster Recovery Strategy is created which caters for complete loss of each major facility (i.e. Office, Datacentre, Cloud capability) and describes a course of action for each scenario, which is then tested.

### 4.7 Business Continuity

To Be Developed in line with 5-year roadmap

### 4.8 Application Strategy

As an application's associated infrastructure approaches end of life, we will undertake the following process to determine next steps:

- 1) Evaluate – Analyse the application and understand whether it still meet's Estyn's needs, or whether it can be retired or replaced
- 2) Migrate – If possible and it is still required, move the application to Azure onto virtualized infrastructure.

- 3) Consolidate – Where possible, use shared infrastructure and platform services such as SQL Azure
- 4) Replace – Applications that no longer suit our purpose or cannot work safely on our ICT infrastructure should be replaced with more modern applications
- 5) Retire – Applications which are no longer required will be retired.

#### 4.9 Supplier Strategy

Estyn will aim to use suppliers which provide

- The required expertise
- Value for money
- Geographical suitability where possible
- Knowledge of the sector

And will procure them via existing frameworks such as NPS, Digital Marketplace and ADIRA.

#### 4.10 Telephony

As described in [5.4.6 Cloud PBX](#) Estyn will move toward cloud PBX telephony, which means that fixed line handsets will ultimately no longer be required. Mobile telephony will be used for staff undertaking inspections.

#### 4.11 Print

Current print needs are managed under a lease arrangement which is considered fit for purpose.

#### 4.12 Retention and Disposal

Retention and disposal schedules will start to be applied across the organisation, in order to comply with legislation such as:

- Public Records Act
- General Data Protection Regulations (GDPR)

This will mean that emails will automatically be deleted after twelve months.

Retention schedules for other documents will vary dependent upon their content.

#### 4.13 Assisted Users

Where possible, Estyn will meet the needs of assisted users, both via the systems that are in use, and by the provision of equipment. User's with additional needs will be assessed by an independent company, which will provide recommendations as to the most suitable equipment.

New applications will be WCAG 2.1 compliant wherever possible.

#### 4.14 Support

See [Appendix B – ICT Support Option Analysis](#).

## 5 Governance

### 5.1 Information Strategy Group

The Information Strategy Group (ISG) will update and oversee implementation of Estyn's IS Strategy. The ISG will agree a set of priorities and a schedule of projects in the form of an IS/IT Improvement Programme that will enhance and develop Estyn's technical infrastructure, software applications and IT support services, and deliver new systems to support business processes. Within the constraints of funding available to Estyn we will continue to invest in information technology to improve efficiency and reduce ongoing business processing costs. There may be the need for certain trade-offs during the period of this strategy in order to focus on particular priorities which best support business requirements, for example, there may be some trade-off between usability and security or between cost and speed of delivery.

The ICT Strategy will continue to be delivered using a business-case/change control process which identifies needs, evaluates options, specifies clear requirements and provides robust cost-benefit analysis. The overall approach will be to seek to maintain flexibility, e.g. avoid tie-in to long-term commitments so that advantage may be taken of any emerging technologies and cost-reductions. Where appropriate, the approach will encompass the use of pilots and trials to de-risk projects so that Estyn only invests where a solution is proven in terms of functionality and can clearly demonstrate business benefit and value for money. Changes and upgrades to systems will be managed through scheduled releases in which we will seek to capture and address a number of consolidated new requirements rather than adopt a piece-meal 'on-the-fly' approach. Funding for new system developments and enhancements will be approved based on an assessment of competing business priorities. We will use an Agile approach to inform decisions based on business value. Preference will be given to developing systems using open standards to enable interoperability. We will fully-evaluate the pros and cons of customising commercial off-the-shelf systems (COTS) to meet business processes against designing business processes around out-of-the-box features of selected software.

### 5.2 Information Services Team

The Information Services team (IST) and Estyn's IT suppliers (partners) will support the delivery of Estyn's objectives by being customer focused, proactive, innovative, organised, flexible, and responsible. Estyn will continue to outsource IT support for end-users and for the maintenance of its network and associated servers but will retain a small in-house capability for end-user IT developments and project management, whether or not contractors carry out the major element of systems work. This will ensure Estyn keeps knowledge and control of key systems, is able to work flexibly to meet most requests by Estyn users and can minimise the cost of external development and support to that of '3rd-line'(high technical knowledge/skills) engineers. Opportunities to make use of shared services to drive cost savings, including sharing applications with others in the public sector (e.g. Joint Inspectorate projects), will be explored. For example, Estyn will use forums such as the Directors of Finance Group for Welsh Government Sponsored Bodies, to benchmark services and identify potential synergies.

## 6 Annex A – Cloud Options Analysis

### 6.1 Types of Cloud Service

There are a number of different types of cloud computing, and it is worthwhile describing them:

**Software as a Service (SaaS)** – A software vendor provides access to their product over the internet. All hosting, operating system management, servers, networking etc is taken care of by the vendor. The Office 365 suite is an example of this.

**Platform as a Service (PaaS)** – A vendor provides the platform, storage, servers and networking, and the user manages the applications and data on this platform. Examples of this are parts of Azure such as Webapps, SQL Azure.

**Infrastructure as a Service (IaaS)** – This gives the ability for virtual servers and virtual infrastructure to be created in an environment where the underlying physical hosts are managed by the provider. Examples of this include MS Azure and AWS for virtual server hosting.

It is to be noted that these types of cloud computing are not mutually exclusive, and organisations may implement all three varieties simultaneously, dependent on their needs.

As is evident from the descriptions, each flavour of Cloud requires a different level of management overhead, and also each flavour of cloud differs in the level of benefit it provides when compared to a traditional on premise, or managed physical architecture. However, many of the benefits apply to all three versions, so this document will focus on those.

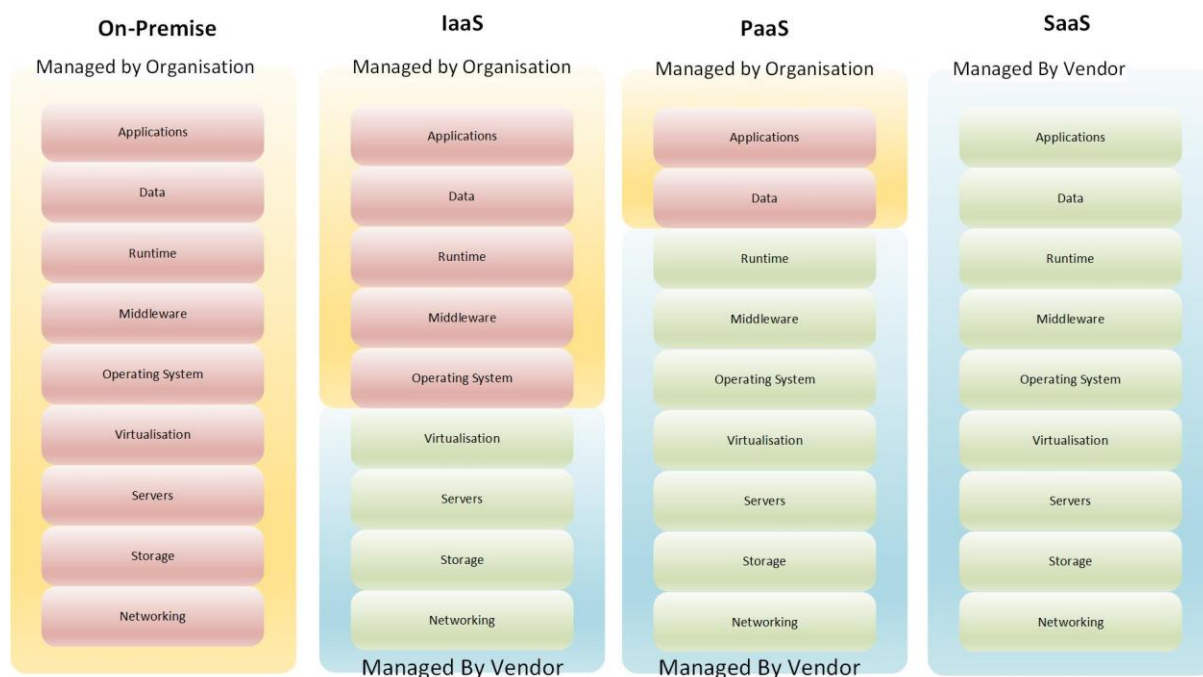


Figure 6 - Types of Cloud Service and division of responsibility

## 6.2 Marketplace Analysis

### 6.2.1 Comparison of Cloud Services

Estyn are considering building the capability to use a Cloud infrastructure when required to allow them to extend their capability and replace deprecated equipment. It will likely result in a reduced TCO (total cost of ownership) regardless of which platform is chosen) and reduced maintenance and upkeep as these are undertaken by the vendor. It will also substantially reduce the capital investment cycle of infrastructure refresh, whereby we need to replace Servers and other equipment periodically (typically 5-7 years). Cloud Services will also provide us with substantially greater resilience, a much-reduced carbon footprint and improved backup capability.

The three largest and most established cloud services vendors in the marketplace are Microsoft Azure, Google and Amazon Web Services (AWS)

As part of the process of picking a strategic cloud provider to provide IaaS and PaaS services, this document will draw comparisons between these vendors, specifically in the context of Estyn's requirements.

### 6.2.2 Comparison Methodology

The purpose of purchasing a cloud solution is to provide a virtual datacentre facility, leveraging the benefits of cloud solutions and reducing total cost of ownership, and reducing the need for capital investment for infrastructure refresh and the perpetual manual maintenance associated with physical infrastructure.

This section will compare the main available cloud vendors against the following criteria

**Compatibility** – Estyn currently have predominantly Microsoft based platforms, and SQL databases. Any solution will need to be able to support these platforms.

**Flexibility** – the solution will need to be flexible to cater for future requirements, such as the delivery of digital services to others, integration to Office 365 and the demands of scalability and performance.

**Ease of migration** – The solution will allow us a swift migration path in order to reduce migration project costs.

**Resilience** – The cloud solution will provide greater resilience to the Estyn estate and have high levels of availability.

**Security** – Estyn's data will be held securely in the cloud, and our infrastructure will have strong perimeter controls to protect it.

**Cost** – We will compare the comparative cost of cloud providers

### 6.2.3 Compatibility (with current and future estate)

Estyn is primarily a Microsoft Server based estate, with a number of COTS (Commercial Off the Shelf) products that depend on the Microsoft platform. Typically, Microsoft SQL Server is used as the standard RDBMS (Database Platform); Most applications run on virtual servers hosted on physical Wintel infrastructure in Estyn's two datacentres.

Google Cloud uses MySQL and NoSQL to provide its data stores and does not support either Oracle or Microsoft SQL Server. At time of writing it does not support Microsoft Operating Systems either, which would mean a re-platforming exercise, which would be a monumental undertaking in an organisation of this scale. On basis of compatibility, we can rule out Google Cloud as a contender at this stage.

Amazon Web Services does provide Virtual Machines using Microsoft Operating systems covering platforms from Server 2003 R2 to 2016. They also support Microsoft SQL Server and Oracle databases, amongst many others.

Microsoft Azure provides the VM capability we would need along with Microsoft SQL compatibility across multiple different versions. In addition, they provide an "Azure SQL" service which provides a lower maintenance, lower TCO (although less configurable) SQL Service, which would likely be suitable for many of Estyn's applications.

### 6.2.4 Flexibility

Both Azure and AWS can provide instant increases in capacity and have the ability to provision services very quickly (within a few minutes). There are multiple options to provide storage solutions in both, which are comparable and provide balances between cost of storage, speed and availability. Azure is better suited to providing hybrid cloud solutions (where a network can be made up of both physical and cloud devices). This would suit Estyn better in terms of migration, as the movement of physical to cloud servers would be a gradual process, rather than a "big bang", therefore the ability to extend Estyn's existing network into the cloud would provide a seamless experience for users, who would be agnostic as to whether they were consuming services on legacy physical servers or new cloud-based servers.

AWS is very well suited to delivering Web Based services with publicly available data. Similar services are available through Azure, but it is considered that these require slightly more configuration. However, due to the product set involved and the current skillsets available, it is likely that Estyn would be better able to manage an Azure environment which provided external services rather than an AWS environment.

AWS is better suited to using Linux third party open source tools than Microsoft Azure, however Estyn use very few of these on the estate and it is not currently on the roadmap to migrate to these, as core platforms.

To summarize, it is very simple to have the Microsoft suite of products available swiftly in Azure, but it can take some time to do any other platforms, the converse is true with AWS.

### 6.2.5 Ease of migration

As the network could be extended via a point to point VPN (Virtual Private Network) into Azure, it would be possible to migrate servers very simply from virtual servers on a physical device, to virtual

servers on a cloud device. Azure integrates well with System Centre and Active Directory, meaning Estyn would not require any additional logon credentials for users. The VPN extension would also mean Estyn could provide either cloud or physical applications to the users, without the user realising the difference. Similarly, application servers in the cloud would be able to access database servers in the physical environment and vice versa. This would mean applications could be migrated to the cloud in stages despite interdependencies with other systems, meaning a much simpler migration and substantial reduction in risk and cost.

Whilst AWS can use a VPN to extend an existing data into the cloud, it does not provide a lot of support for the physical environment and does not have the simplicity to integrate with tools such as Active Directory. Consequently, it is likely that large groups of applications (if they were co-dependent) would need to be migrated simultaneously, requiring more extensive planning and testing than if they could be migrated independently, therefore incurring greater costs and longer timeframes.

### 6.2.6 Resilience

In Azure, servers are constantly monitored for faults by a system called the Azure Fabric Controller. Should a fault be detected on a virtual machine (either in the hardware or the underpinning software) then the virtual machine is automatically relocated.

In terms of storage, Azure maintains three replicas of all blob (Binary Large Object – a document, graphic, PDF or other type of file), table and queue data. It also allows the option of geo-replication to store backups of blobs and tables in a secondary datacentre. Azure operates datacentres in many parts of the world, so if required, geographic resilience can also be implemented. However, the most likely scenario for Estyn would be to deploy to two different UK datacentres. The Azure datacentres are highly resilient, so even this approach may be deemed overly risk averse for certain applications, especially as the move away from physical infrastructure removes many of the risks which justified the use of multiple physical environments.

These application availability features include the blob snapshot feature to create point-in-time backups of blob data.

AWS also provides multiple availability zones in data centre regions, meaning applications will failover between datacentres within regions. In addition, multiple regions can be utilized to provide geographic resilience.

### 6.2.7 Security

Microsoft have two UK based Azure facilities, so any concerns regarding legal jurisdiction are satisfied. Amazon also have two UK based datacentres.

In terms of security infrastructure, both platforms have a good track record of defending against cyber-attack, with no major incidents recorded. Facilities such as encrypted SSL traffic, logical traffic separation and active threat detection and management are standard across both platforms. Azure can also offer Multi Factor Authentication for users (as well as linking to Active Directory) however it is unlikely we would use these functions as remote users would probably connect via a remote worker VPN service into the network and bridge across to the cloud. Further security due diligence specific to Estyn will be undertaken during the design phase of the project.



### 6.2.8 Cost

Amazon Web Services is generally slightly cheaper on a server for server basis, however when using Microsoft software/services on Azure, there are substantial cost incentives compared to other cloud vendors, and a huge reduction in TCO compared to traditional infrastructure. Both environments have complex layers of service and support available and comparing all the permutations would be expansive, however, Microsoft specific support is available at different levels via Azure, which would be particularly beneficial to Estyn as this would cover the vast majority of its platform. Initial costs to connect to each environment would be very similar

### 6.2.9 Summary

The services available from AWS and Azure are highly competitive. As such, there is little to choose between them in terms of functionality and price. However, there is a clear advantage in Azure with regard to the easier migration path, the support available with regard to Microsoft products, the relevance of existing skillsets within Estyn and the marketplace and integration with on-site software and infrastructure during a migration phase.

The other advantage in favour of Azure is that its UK West datacentres is in South East Wales. Local datacentres mean a reduced latency and improved performance for users (as networks have less far to travel) and also ensures that data stored in the cloud is protected by UK legislation.

### 6.3 Option Analysis

As a consequence of section 2, the following options only consider a potential move to Microsoft Azure's datacentre.

#### 6.3.1 Option 1 – Do Nothing (stay on premise)

This option means continuing with an on-premise deployment

##### **Benefits**

Easier to fund, in terms of availability of Capital funding vs Revenue funding

Predictable costs

##### **Disadvantages**

Not resilient between datacentres

Capital investment required as some equipment is ageing

No flexibility – once equipment is purchased it is there for its lifespan

Long turnaround in terms of purchase and commission of new equipment

No scope to save money from turning down environments on weekends and evenings

Lower levels of resilience

#### 6.3.2 Option 2 – Move all systems to Azure Cloud capability

This option would mean commencing a large programme of work, to begin moving all Estyn's systems to Azure within a timeboxed period

##### **Benefits**

- Will result in all the estate benefitting from the resilience of the cloud
- No more Capital infrastructure refresh cycles once migration is complete
- Increased resilience

##### **Disadvantages**

- Investments already made will become nugatory expenditure if they are decommissioned early
- Some applications may not be suitable for the cloud
- A large amount of change will be required by Estyn Staff at a time when there will already be business changes as a result of the Donaldson review
- There is a substantial initial investment required

### 6.3.3 Option 3 – Enable Cloud capability

This option means enabling the building of cloud capability – i.e. extending Estyn’s network into the Azure cloud datacentre facility, which then allows the seamless provision of cloud services, as and when Estyn feel it is appropriate to do so.

#### **Benefits**

- Small initial cost to develop the capability
- Provides options going forward either to leverage cloud or continue on premise
- Allows Estyn to experience the cloud without making a large commitment
- Enables a gradual cloud migration, rather than the risks of big bang

#### **Disadvantages**

- The cloud capability will require a small amount of management

### 6.4 Recommendation

Estyn are currently interested in exploring the use of Cloud services, in line with Government guidance and other public bodies. As oppose to a wholesale migration programme, this paper recommends considering the use of cloud for each new service that Estyn require, or for each service that needs to be replaced due to the age of its infrastructure of if a more up to date platform is desired – as per Option 3. It is recommended that Estyn build an Azure tenancy and then seek to move services into the cloud if and when required, in a gradual migration, which will leverage the investment currently made in on-premise infrastructure, whilst allowing the progressive move toward cloud.

## 7 Appendix B – ICT Support Option Analysis

### 7.1 Purpose

This paper details ongoing options for day-to-day ICT support (otherwise known as Business As Usual or BAU) for Esytyn. BAU ICT Support usually consists of the following components, (although some or all of these may or may not be provided by a supplier, dependent upon in-house capability)

- Service Desk – first point of contact for handling incidents, requests and queries from users
- Server and Storage Management patching and maintenance including fix on fail
- Desktop Services – Ensuring patching and AV are up to date as well as deploying updates of core applications as required
- Capacity Planning and Monitoring – Monitoring current capacity and ensuring there is sufficient capacity for growth
- Cyber Security monitoring – protecting against cyber-attacks and responding when they do occur
- ICT Asset Management – Tracking all purchased ICT Assets, including desktop PC's, phones, servers, laptops and licenses
- Application Support – Providing support on the organisation's applications (this is sometimes outsourced to the application vendor)
- Network/Infrastructure support – Ensuring network work devices are working correctly, fixing them on failure and ensuring they are patched appropriately
- Change Management – Managing any changes required to the ICT Estate in a controlled manner, in order not to cause disruption

### 7.2 Background

Estyn have currently used the same ICT Vendor, Westgate IT for the last 9 years to provide their BAU ICT Service. The contract is due to end in August, and the current value is approximately **100k per annum.**

Estyn are currently developing their 3-5 year ICT Strategy, including how the mainstreaming of Cloud technology could offer multiple benefits in terms of resilience, maintenance, flexibility and security. Therefore, it is timely that future ICT Support considerations are now undertaken.

## 7.3 Option Analysis

### 7.3.1 Option 1 – Do Nothing

This option means letting the current contract expire and proceeding without ICT Support.

#### **Benefits**

- Short Term Cost-saving

#### **Disadvantages**

- Gap in ICT support capability
- Vulnerability to Cyber Attack
- No support for staff
- Outdated server patching
- Asset Management will swiftly become out of date
- No means to fix failed servers, services or devices
- High risk to Estyn’s organisational resilience

### 7.3.2 Option 2 – Re-procure Existing Supplier

This option would involve either extending the current Westgate IT contract, or letting a new direct award contract to them, which would likely require a procurement process departure note. It is anticipated that this would incur a similar or slightly increased cost.

#### **Benefits**

- Continuity of Service
- Provider is a known quantity
- No transition to another supplier required

#### **Disadvantages**

- Likely to be in breach of procurement law for Public Sector bodies.
- The service may not provide adequate support for new technologies such as cloud, as currently contracted
- Some failings of the current service have already been noted, such as failure to patch, and failure to maintain SQL databases.

### 7.3.3 Option 3 – Procure a new Support agreement

Undertake an open or framework-based procurement to procure a new ICT Support Service. It is anticipated that costs would be broadly similar to what Estyn currently pay. The first step would be for Estyn to detail their current and future requirements for support, to ensure that any new service will enable the organisation to meet its corporate goals and the milestones in the ICT Strategy.

### Benefits

- Allows Estyn to ensure any new service caters for any potential move to cloud
- Ensure up-to-date competitive pricing
- Compliant from a procurement perspective
- Modern support contracts more likely to have a focus on cyber security
- Estyn can write up their current and future requirements, rather than having a service that meets their old requirement – making this a strategic service
- Predictable levels of expenditure
- Guaranteed levels of service

### Disadvantages

- Can be inflexible
- Services can contain hidden costs, for example for change requests

#### 7.3.4 Option 4 – Build an in-house ICT Service

Currently Estyn has two members of staff with ICT Support capabilities. This would mean creating a new capability within Estyn, to manage the entire ICT Service. It is estimated that this would require an additional 4 full time staff as a minimum, in order to cater for leave and sickness absence and ensure continuity of service. It is to be noted, that these 4 members of staff would need to have a medium level of expertise and generalist skills. As-and-when expertise would need to be purchased periodically, as it would not be financially viable to employ high level ICT experts on a permanent basis for an organisation of Estyn’s size and complexity.

Estimated costs as follows:

Description	Cost	Total
<b>4 x Permanent members of staff</b>	£30,000-35000 per employee, with on-costs	£120,000 – £140,000
<b>Expert Resource as Required (20-30 days estimated)</b>	£800 per day	£16,000 - £24,000
	<b>Total</b>	<b>£136,000 - £164,000</b>

### Benefits

- Mostly Predictable spend
- Estyn can control the ICT function and change it as required

### Disadvantages

- Service not guaranteed (multiple staff illness)
- Staff may leave which can cause a gap in service
- May be difficult to procure appropriate permanent staff
- May be difficult to find expert resource at short notice, if required urgently

#### 7.3.5 Option 5 – Use a Public Sector Shared Service

There are currently few Public Sector Shared Services available which Estyn may be able to subscribe to that would meet all its requirements. These Shared Services are typically created by groups of Public Sector Bodies which have common architecture and goals, in order to be able to share costs. It is difficult to forecast costs, however as typically Shared Service.

#### **Benefit**

- Costs can be shared with other users of the shared service

#### **Disadvantages**

- Due to size, Estyn is likely to be a small player in any Shared Service and therefore unlikely
- Support services are quite generalized and support for specialist applications could be limited
- Resources are shared amongst much larger partners with more critical systems, meaning Estyn would likely be de-prioritised.

#### 7.4 Recommendation

On analysis, the recommendation for Estyn is Option 3. Only this option provides:

- A guaranteed level of service
- A service that is aligned to Estyn's strategy
- A predictable level of spend
- A competitive and compliant procurement

# Corporate Services Structure

