Transforming digital continuity

Enhancing IT resilience through cloud computing

A joint research report

Prepared by

Estonian Ministry of Economic Affairs & Communications and Microsoft

May 2016

Table of Contents

In the years since its 1991 re-independence, Estonia has built a robust information society from the ground up. Now, more than two decades into Estonia's experiment with e-government, the e-solutions developed in the 1990s and 2000s are pervasive. Estonians enroll in school online. They apply for social services online. 30% vote online. Estonians can do everything online, apart from getting married. More than 95% of information is digital. One might forget how to manually sign documents because in Estonia only digital signatures are used. This way we have saved an estimated 2% of GDP. For many important state registries, like the Land Register, there are no paper backups or copies. Digital is it. It is not just Estonian citizens and residents who rely on our digital infrastructure. Estonia's e-Residency program allows anyone in the world to take advantage of our convenient digital services by becoming an "e-Estonian." Via the initiative, thousands of people have used Estonia's e-services to establish and run companies, or just make managing their everyday affairs easier. We call this philosophy country-as-a-service. The idea is simple: not only do we want to offer our people excellent digital services, by making our easily-scalable e-services available to those outside of Estonia, we will expand global access to secure, transparent, and efficient digital services.

Estonia's use of e-services has improved the country's prosperity and the well-being of its citizens and e-residents. At the same time, our radical dependency on these technologies presents risks, some of which are relatively unique to the digital context. If the integrity of the databases and algorithms behind our electronic ID card system was compromised, for example, key aspects of Estonian public life and government would be entirely unable to function. For Estonia, then, "digital continuity" and "government resiliency" are not just "policy speak". Our business sector, civic sphere, and citizens' private lives are all intertwined with, and reliant upon, our e-services and systems. Yes, our bureaucracy depends on this infrastructure, but so do our economy and society.

Estonia has made concentrated efforts to ensure that vital services, those essential to the enactment of Estonian statehood and the well-being of our citizens—like our electronic ID system and Land Register—can not only withstand cyber-attacks, but also function, or at a minimum endure intact, in the face of natural disasters or even conventional warfare. Geopolitical turmoil in 2014 brought into stark relief the necessity of these efforts.

The agility afforded Estonia by its size and lack of legacy systems has enabled it to be an e-government bellwether. As more and more countries follow Estonia in digitizing the databases, registers, and identification systems that make governance possible, the risks and challenges Estonia faces will become more widespread. Thus, in sharing our experiences dealing with the policy questions and technical challenges involved in running an Estonian registry from the public cloud, our aim is not to simply present an anomalous case study from the northern corner of

Europe and the vanguard of e-governance. Rather, we hope that these findings will be useful both for companies that offer cloud computing services and want to learn more about how to best serve the needs of public sector clients, and for government officials around the world looking to safeguard the functionality and continuity of their states in the cloud.

Taavi Kotka
Estonia Government CIO

Earlier this month, Marketwatch noted that Estonia, a Baltic country of just 1.3 million people, is the most technologically advanced in the world. "In Estonia, voting, signing documents and filling out tax returns is done online, thanks to…an online tool that coordinates multiple online data repositories and document registries. Estonians…have unparalleled access to the data they need to do business, get licenses, permits and other documents that would take days, weeks or even months in other countries."

And all that government data needs to be safe and available through any disruption.

Who better to develop and test such continuity capabilities than Estonia? And working with Microsoft, a partner equally committed to security, could it be shown that the resilience of a digital government's services can be significantly enhanced through the use of public cloud?

We focused on the Estonia Land Register, the official record of land ownership. We tested whether this particular government service could successfully failover to the public cloud, in this case Microsoft Azure, and continue to operate from the cloud, especially when such a need arises. Instilling confidence and trust in the long-term sustainability and integrity of government services is important to every society. Below are the results of the research, jointly published by the Estonia CIO and Microsoft.

Private and public organizations all over the world are embracing modern technologies in new and unprecedented ways. Cloud computing enables entities to increase productivity, and reach unprecedented scale, either by using pre-packaged solutions or building on top of the platform to provide their own services. For governments in particular, digital transformation can unlock service delivery unimaginable even a few years ago – helping them better serve their communities every day.

Anand Eswaran
Corporate Vice President, Microsoft Services

1 Executive summary

This joint research report, drawn together by the Estonian Ministry of Economic Affairs & Communications and Microsoft, addresses how public cloud computing can enhance government digital continuity. In other words, it looks at the role commercially delivered cloud computing can play in giving a state the capacity to maintain its government services and the data it needs to function, regardless of adverse developments and crises.

The aim of this report is to help policy makers and civil servants better understand the policy and technical implications, benefits and limitations of incorporating such public cloud computing into governmental digital continuity plans.

Since late 2014, the Estonian Ministry of Economic Affairs & Communications and Microsoft have been addressing the question of cloud resilience in a multi-phase joint project. Phase I having addressed proprietary government clouds and virtual "data embassies", Phase II looked at the use of public cloud for resilience in a crisis. This report deals with Phase II, which concluded in May 2016.

Incorporating public cloud into a state's digital continuity plans presents potential risks and benefits. As states' operations become more data-driven and ICT-centric, ensuring those operations are as resilient as possible becomes increasingly relevant. Governments' options for ensuring resilience have potentially been greatly expanded by the emergence of hyperscale cloud computing infrastructure. Nonetheless, there remain challenges that should be addressed so that this potential can be realized. Alongside the technical complexities of achieving an important government digital service's "failover" into the cloud during a crisis, there are policy complexities to be addressed by any state preparing to transfer its data and/or the data of its citizens outside of its borders (this geographical distribution over multiple data centers in different jurisdictions, indeed across different continents, being one of the fundamental ways the cloud achieves its resilience).

Following the approach taken during Phase I, a number of policy and technical hypotheses were developed by the Estonian and Microsoft team. These eight Phase II hypotheses (see Table 1) were tested as part of the technical trials and policy discussions.

The focus of Phase II was to create a limited cloud resilience "proof-of-concept" environment for Estonia's Land Register, an important government system that is wholly digital. This proof-of-concept would model the type of geographic failover capability that could protect a service such as the Land Register from the consequences of a major crisis, e.g. a natural disaster, a critical infrastructure failure or a significant attack. The proof-of-concept was successful, and along with the testing of the eight core hypotheses, it produced a number of technical and policy findings and recommendations. Central to these were the importance of establishing a digital continuity principle within disaster planning, building trust-based partnerships between states and private sector cloud providers, and preparing ahead of any crisis both the technical basis and the policy basis for harnessing cloud in the name of a state's digital continuity.

Core Hypothesis: Public cloud enhances digital continuity for government services. Additional hypotheses were tested (see Section 8), addressing technical and policy aspects of using public cloud for resilience in the event of a crisis. The following table summarizes the outcomes of that testing process.		
Area	**Policy aspects**	**Technical aspects**
Key findings of the research project	Digital continuity principles, strategy, and failover procedures are likely to require periodic review, as technologies continue to evolve.	Digital continuity for government services in a public cloud offering is technically possible for most modern applications, however the underlying operating system, data platform and availability architecture typically requires re-evaluation and potential modernization to be achieved.
Key challenges	Technology is developing at such a rapid pace that existing policy frameworks will continue to require updating in order to enable an appropriate, secure and expanding use of public cloud failover for prioritized government services. There is also "trust gap" around public cloud in terms of security and transparency that is best addressed between cloud providers and government. The consequences of exposing or losing citizens' private information may be hard to measure and therefore difficult for governments to provide appropriate restitution.	While similar in nature, public cloud infrastructure platforms have different requirements and characteristics than that of on-premises architectures. These differences may impact the speed and level of effort required for a given application to support digital continuity within the public cloud. This requires an investment of time to support testing, evaluation and sometimes troubleshooting to provide an application infrastructure that is functionally equivalent to that of on-premises. In some cases, an application's platform services must be reconfigured or updated to enable a level of required support before it can be moved to the public cloud.
Key recommendations	Digital continuity principles, policies and programs are a necessity for any modern government agency or department. Governments should establish a prioritized list of services that must maintain digital continuity in all circumstances. Governments should ensure that the on-premises applications and platforms they rely upon are modern standards-based and can transition to cloud. A risk assessment should be conducted for each class of data and government service if a migration to a public cloud is considered.	To support digital continuity strategy that includes public cloud, a Technical Dependency Analysis (TDA) must be performed on the application or service which is being protected. Once complete, operational procedures and dependent infrastructure should be deployed, prepared and tested in advance to failure events to be effective. Operational procedures and dependent infrastructure should be deployed, prepared and tested in advance to failure events to be effective. Apart of risk assessments, the responsibility for risk acceptance must be clear. Without knowing the consequences of accepting a risk, that person may be exposed to unforeseen risks.

Table 1: *Summary of Phase II Hypotheses*

In conclusion, Phase II of the joint research between the Estonian Ministry of Economic Affairs & Communications and Microsoft, successfully advanced both parties' understanding of what is feasible in terms of using commercial, public cloud computing to enhance a state's digital continuity and resilience capabilities.

2 Introduction

Estonia has created one of the world's most advanced digital societies. Key aspects of state infrastructure and Estonians' everyday lives are heavily technology-dependent: Estonians have provided more than 282 million digital signatures,[1] nearly all of the medical prescriptions in Estonia are electronic, and crucial government databases, such as the Land Register, exist exclusively in electronic form. With the convenience and cost-effectiveness of a robust digital society comes an unprecedented sensitivity to cyber-attacks and disruptions. Indeed, attacks on Estonia's information and communications technology (ICT) infrastructure have the potential to both damage state infrastructure and hinder the normal functioning of public and private life.

Estonia is one of the global leaders in the field of cybersecurity. In 2008, Estonia was among the first countries in the world to adopt a National Cyber Security Strategy and in 2014 a new Cyber Security Strategy for 2014-2017 was signed. This 2014 strategy highlights digital continuity as one of its strategic goals, but only mentions cloud computing in passing. Indeed, few governments anywhere have looked specifically at the question of how public cloud computing can enhance government digital continuity, including ensuring that government services can continue to function securely and with integrity in the face of a significant natural disaster or cyber-attack.

Since late 2014, the Estonian Ministry of Economic Affairs & Communications and Microsoft have been addressing this question in a multi-phase joint project. Phase I, completed in early 2015, focused on testing non-critical services and their migration to the public cloud. The Phase I Report (available here) recommended that:

- An overarching cloud strategy and government action plan facilitating cloud migration should be developed to enable technical and operational agility and increase cost-effectiveness;
- Cloud computing should be used to increase security and resilience of government infrastructure; and,
- For the migration of restricted data, countries should consider developing digital continuity legislation and a strategy to increase assurances of diplomatic and other international law protections.

The Phase I Report also described two potential ways in which states could harness cloud computing to advance their digital continuity goals: proprietary government clouds and virtual "data embassies."

In late 2015, the Estonia Ministry of Economic Affairs & Communications created the Estonia Cloud Action Plan with assistance from the Information System Authority and others. This Action Plan included the Estonia private cloud, with a minimum of two different physical locations, and the use of public cloud and data embassies located outside of Estonia. Core drivers for the Estonia Action Plan include: 1) digital continuity (resilience); 2) mitigating information technology risk, including by enhancing information security capabilities; 3) contributing to high quality and innovative e-services; 4) increasing cost-

[1] Statistics available here: http://id.ee/

effectiveness (e.g. every state authority does not need to obtain server hardware nor locate it in two different locations, because this is all done by one operator of the government cloud, who optimizes the use of state resources); and, 5) assisting state authorities in complying with procedures laid down by the acts regarding information systems and the security thereof.

Phase II of the project, completed in May 2016, focused on agreements with public cloud service providers, looking at the feasibility of a critical Estonian government service using public cloud for resilience in the event of a crisis. This Phase II Report documents both the efforts of the joint technical work (which involved running a copy of Estonia's Land Register from Microsoft's public cloud platform) and also the outcomes of policy discussions. Its aim is to help policy makers and civil servants better understand the implications, benefits and limitations of incorporating commercial public cloud computing into governmental digital continuity plans.

3 Digital continuity in government resilience

Digital continuity means the capacity of a state to maintain its services and digital data relevant for the functioning of the state, regardless of any adverse changes or interruptions.[2] It includes processes that enable stability, ensure recovery and help restore government services rapidly in the event of a crisis or natural disaster, so that those services can continue to be available and operate without being compromised. The potential role of cloud computing in enhancing digital continuity is a comparatively recent consideration for many states. However, building on a trend several decades in the making, governments have increasingly taken advantage of new technologies. Processes that might have taken weeks can now be done in days, hours and, sometimes, minutes. Indeed, in some countries, not least Estonia, many state services now exist primarily, or only, in digital format. These services can often be critical to the functioning of the state or to citizens' ability to exercise their constitutional rights. Maintaining those services, especially in a crisis, is a core function of the state and this requires innovation in cybersecurity thinking, not only regarding increasing cyber threats but also regarding potential impact of natural and man-made disasters and threats. Incorporating public cloud into a country's digital continuity plans presents a series of potential risks and benefits. Determining the optimal extent and scope for reliance on public cloud will depend on the risk appetite and threat landscape in a given country. Differing locations bring differing geopolitical and environmental risks. Differing national infrastructures and *modus operandi* pose distinct challenges. The range of options realistically available to a state is contingent on its economic, social, political, legal and bureaucratic context, while divergent technical capabilities make some responses more or less feasible.

More than this, the incorporation of public cloud into digital continuity is further complicated by states' different assumptions (largely unexamined until now) about what can be done with the data that sits at the heart of government systems. Can data that resides in a particular state be transferred outside of its territory? If so, where to? What does a government system's "failover" to the cloud look like? Which statutory authority or agreed procedure determines when this happens and how? How can the state ensure that data is being handled in a responsible and secure manner outside of its jurisdiction? Is data outside of a state's jurisdiction if it resides in the cloud or in a "virtual data embassy"? In extreme situations, can critical state functions, e.g. legislating or identifying property ownership, be moved to the public cloud, even outside a country's physical territory and how can this be secured in a way that meets public expectations of privacy?

These policy complexities have to be addressed alongside the technical challenges that come with creating critical systems for states that are capable of genuine digital continuity. Many of these questions require a broad discussion within the society, incorporating technical, legal and political perspectives. The reward for states that meet these challenges will be the ability to maximize not only the benefits of ICT for its operations and services, but the wider opportunity to support and enhance digital continuity plans through the application of cloud computing.

[2] Kotka, Ainge, Kask, Lellsaar (2016) The Concept of Data Embassies – Safeguarding Digital Continuity, *publication pending*.

4 The role of cloud computing in digital continuity

As states' operations become more data-driven and ICT-centric they must ensure that their services and data are as resilient as possible, and can be, if needed, restored quickly in times of crisis. One possible solution is the use of public cloud to improve existing digital continuity plans, as well as to support well-established approaches to disaster response and recovery. The emergence of hyperscale cloud computing infrastructure greatly expands the options a government has for ensuring that the digital continuity of key services are not geographically bound.

A range of issues, from jurisdiction and security of citizens' data through to the need to build genuine trust with public cloud providers, have to be addressed before governments can move forward. In this paper we set out to explore how public cloud can contribute to delivering digital continuity for states by virtue of being distributed, scalable, and cost-effective.

4.1 Geographically dispersed datacenters

Most specific risks, e.g. earthquakes or flooding, tend to be concentrated in particular locations or geographies. Major cloud service providers, however, typically run multiple datacenters across several different locations, states and continents, and then replicate customer data and workloads in two or more locations. This allows them to provide robust service levels and data resilience in the face of geographically focused risks. As one expert has noted, protecting against data loss "is the objective of [having] geographically separated, secure, duplicate, redundant computing services. Commercial cloud service providers know very well what has to be done to maintain continuity of operations under just about any known conditions…"[3]

This geographical dispersal may bring with it problems when data is no longer stored under the legal system of the original state. The status of government data in a dispersed public cloud has not yet been tested in courts and therefore this potential jurisdictional risk needs to be considered.

Should the jurisdictional risk be addressed to the satisfaction of government and the public, geographical dispersal could allow cloud providers to offer much higher levels of availability and resilience than most public-sector organizations can achieve on their own, especially smaller organizations with a limited number of servers that are all situated in a single location.

4.2 Scalability

Cloud services can provide colossal levels of computing power effectively on demand, meaning that government departments and agencies can use these services as fail-over for their own systems, as and when needed. Taking full advantage of this would, however, require the relevant government system to

[3] Paul Wormeli, IJIS Institute, *Mitigating Risks in the Application of Cloud Computing in Law Enforcement* 22 (2012), available at http://www.businessofgovernment.org/report/mitigating-risks-application-cloud-computing-law-enforcement.

maintain active contracts with cloud service providers and to keep a skeleton-version of the infrastructure running in the cloud. This would have funding implications.

Because certain government data and services are likely to be in particularly high demand during times of crisis, the highly scalable and "elastic" nature of cloud computing means systems supporting these services are less likely to crash, even under unusually heavy usage requirements. The Organization of Economic Cooperation and Development (OECD) has noted, that the "elasticity" of cloud computing is one of its great strengths: "Computing resources can be provisioned in an elastic and rapid way that allows adaptation to changing requirements such as the amount of data supported by a service or the number of parallel users."[4]

4.3 Cost-effectiveness

Most public cloud services are available on an as-used, pay-as-you-go or subscription basis. Specific public procurement processes would need to be accounted for but in theory governments could use public cloud to avoid having to invest substantial resources in purchasing, building, and maintaining their own systems, only to see them sit idle most of the time. For these reasons, in some contexts, "using the cloud as a [disaster recovery] platform makes it more affordable to create a truly durable implementation by replicating systems and data across multiple geographies."[5] Whether a subscription to a public cloud service would be cost-effective will depend on an analysis of these advantages and potential extra costs. Such costs include the necessary rebuilding of the architecture for those services, the maintenance of duplicate services (on premises and in the public cloud) and training staff to manage a more complicated architecture.

Furthermore, provision would need to be made for the costs of using the cloud during a scale attack or a rapid deployment, as they could accumulate rapidly.

[4] OECD, *Cloud Computing: The Concept, Impacts, and the Role of Government Policy* (2014), available at http://www.oecd-ilibrary.org/science-and-technology/cloud-computing-the-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en.

[5] Lauren Whitehouse and Jason Buffington, Enterprise Strategy Group, *Amazon Web Services: Enabling Cost-Efficient Disaster Recovery Leveraging Cloud Infrastructure* 3 (Jan. 2012), available at http://d36cz9buwru1tt.cloudfront.net/ESG_WP_AWS_DR_Jan_2012.pdf

5 Foundations for state use of public cloud

While there appears to a case for the use of public cloud services within state digital continuity and disaster recovery plans, relatively few governments have codified this recognition into formal government-wide policy that encourages the use of cloud services for this purpose. In fact, many states have policies in place that could make it difficult for government departments and agencies to use cloud services in this way. Based on a review of several jurisdictions,[6] including several that have embraced the move to digital data and services in government, we identified several areas that need to be addressed as part of enabling the use of cloud services for government digital continuity and disaster recovery planning. These include:

a. Data residency requirements, in order to set appropriately limited restrictions or prohibitions on transferring or storing public-sector data outside national borders, in particular as relates to national security, and in order to enhance the value of cloud services in continuity or recovery scenarios;

b. Modernized rules and requirements, to enable the use of ICT services rather than rely on paper documentation, in person signatures, on-premises computing systems; to adjust procurement or budget rules that see ICT purchases solely in terms of "one off" capital expenditure (cap ex) and not, as in the case of cloud computing, as an operating expenditure (op ex) for an "ongoing service."

c. Avoidance of replication of services, as states should avoid effectively competing with the private sector for services that already exist and could be bought in as such.

d. Standards-led and internationally aligned security requirements, which will enable cloud services providers meeting international security standards to deliver the services needed.

e. Robust broadband infrastructure, which is a fundamental prerequisite to the successful use of cloud services, especially in the context of disaster recovery.

f. Greater flexibility on auditing by cloud service providers, either by allowing governments to ensure that security standards are followed according to the government's needs or by using a broader range of security certifications to address changes in the technology landscape.

g. Increased transparency between both governments and cloud service providers is required to build and maintain public trust.

[6] Including Australia, Germany, Japan, Korea, Norway, the United States, and the UK.

6 Digital continuity: Relevant beyond Estonia?

The land register proof-of-concept, discussed in Section 7 below, and the particular technical lessons learned are specific to Estonia, but the hypotheses tested by Phase II of the joint research project have wider relevance to all states and agencies considering their digital continuity plans. As technology continues to advance, and as opportunities for using cloud in digital continuity and wider resilience become better understood, the core challenges are likely to remain: 1) whether states will be able to trust in the technology and its providers; and, 2) whether laws enacted pre-Internet can be modified to allow such trust to be acted upon. States should consider approaches to these twin challenges that, like this joint project, embrace a willingness to learn alongside (not only from) the private sector. Equally, public cloud providers will need to adapt their modes of thinking away from "business as usual" to learn from the challenges faced by politicians and civil servants, who must take into account citizens' rights, sovereignty over data, the long-term strategic interests of a nation and a dozen other fundamentals, when developing even the most basic of digital continuity strategies. The approach taken by this joint project demonstrates these truths.

6.1 Estonia ICT principles

Estonia's digital leadership[7] has meant the country is well positioned to deal with the use of public cloud within its digital continuity. Estonia's approach has been based on half-a-dozen ICT principles that have shaped its systems and processes. Although these principles are specific to Estonia, they are worth recapitulating here. The six ICT principles are:

1. **Single digital identity:** Each citizen should at birth be assigned a unique identifier that is associated with that person's rights and obligation within the government framework. This identified should be linked to a secure digital identity that the citizen uses in execution of their rights and obligations.
2. **Citizen control of data:** Each citizen should have control over his or her data and should be given information about how it is being used and when it is being accessed. Exceptions should be allowed for criminal investigations.
3. **Once-only policy:** Government agencies should only collect information from the citizen once and be ready and able to share information with other government agencies, when required.
4. **Central catalog of ICT systems:** All government information systems should be cataloged and registered centrally. Information should be made public to the extent possible.
5. **Mandatory X-Road:** X-Road[8] should represent the exclusive channel for data exchange among different information systems to facilitate the once-only principle.
6. **No legacy systems.** The government should be vigilant to ensure that any government ICT systems approaching the end of their lifecycle, e.g. 13 years, are phased out as soon as possible.

[7] European Commision, 2016. Available at: https://ec.europa.eu/digital-single-market/en/scoreboard/estonia
[8] X-Road, the data exchange layer for information systems, is a technological and organizational environment enabling a secure Internet-based data exchange between information systems. https://www.ria.ee/en/x-road.html

7 Cloud resiliency proof-of-concept

Phase II of the joint research project focused on failing over the Estonian Land Register service into Microsoft Azure. Given the importance of land ownership records to citizens, businesses and the government alike, this service is a prime example of a service the Estonian state requires enhanced resilience for.

7.1 Current state

The Land Register is a multi-tier, web-based application that allows Estonian citizens and business owners to research, purchase, sell and prove ownership over physical property within Estonia. It is the system of record for all land transactions and is completely digital. A conceptual diagram of the Land Register is provided below for reference:

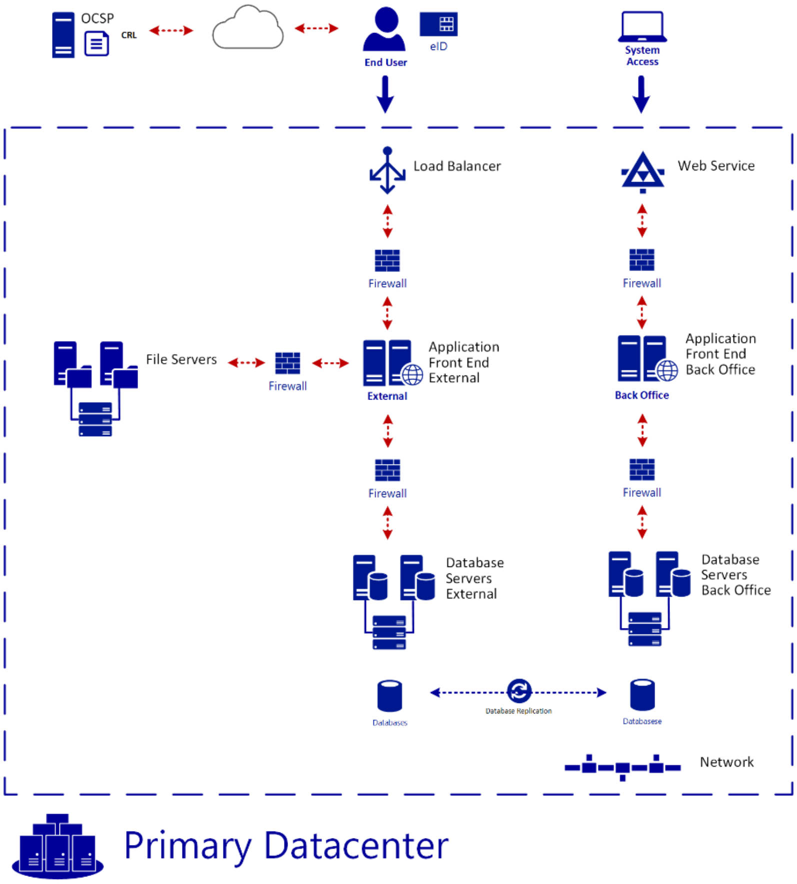


Figure 1: *Proof-of-concept on-premises application conceptual architecture*

7.2 The challenge

Operating a critical public facing service such as the Estonian Land Register involves being prepared for managing system outages, misconfigurations, cyber security attacks and corrupt data. When they happen, these incidents often require focused activities to support return-to-service for the application. There is an explicit assumption that a secondary instance of the application can support operations until the primary instance is restored. The ability to manage and mitigate these isolated disruptions is often what defines an organization's ability to keep a stable, viable and running service.

With today's complex application landscape, achieving continuity of operations can introduce several technical challenges. Rapidly recovering from a major disruption or disaster is critical for most government agencies providing key services for their citizens and such capabilities must be addressed by each organization's resiliency strategy. In this context, the Land Register requires a level of resiliency which necessitates that the application infrastructure span beyond its country's borders, in case the country's infrastructure is severely impaired, e.g. by man-made or natural disaster scenarios. A defined geographic failover capability, which provides protection against major attack vectors and other events leading to disruptions, is a requirement for the Land Register. In an effort to provide this capability without establishing a physical datacenter infrastructure in another geography or country, the Estonian government partnered with Microsoft to support a limited cloud resiliency proof-of-concept environment for the Land Register application, using Microsoft Azure.

7.3 Proof-of-Concept

The Estonian Ministry of Economic Affairs & Communications and Microsoft developed a cloud resiliency proof-of-concept for the Land Register application. The goals of the cloud resiliency proof-of-concept included:

- Testing the feasibility of hosting the Land Register application public part (read-only) on Microsoft Azure cloud platform;
- Testing the feasibility of using other Estonian governmental registration applications which leverage the Estonian X-Road platform[9] and which require services like an Online Certificate Status Protocol (OCSP) front-end and timestamping;
- Testing the process of automated failover from the on-premises datacenter to the public cloud (Microsoft Azure); and,
- Testing the Land Register main functionalities working as required in Microsoft Azure, performance tests were excluded this time.

The Estonia Land Register application currently resides within two datacenters located in Estonia to provide on-premises redundancy. If access to the primary datacenter is lost for whatever reason, systems hosting an up-to-date copy of both the data and application within the secondary datacenter are able to provide business continuity for the service. While this is sufficient to protect against traditional outages, it

[9] https://www.ria.ee/en/x-road.html

does not provide full continuity against man-made or natural disaster scenarios which could impact either datacenters or a large geography within the region. The goal of this proof-of-concept was to validate the ability to host a third site using the Microsoft Azure public cloud, to enable failover in cases where datacenters located inside Estonia's borders may not be able to provide resiliency against the type of disasters which could be encountered.

7.4 Proof-of-concept environment overview

The proof-of-concept environment was set up to use an on-premises datacenter location and a Microsoft Azure subscription. The primary on-premises Land Register infrastructure consisted of a series of virtual machines hosted on a VMWare ESX environment. The secondary Microsoft Azure infrastructure comprised a combination of infrastructure-as-a-service (IaaS) virtual machines and platform-as-a-service (PaaS) services for network connectivity and automation.

The Land Register application's redundancy was provided on two levels. First, the front-end application servers were deployed in a binary-consistent manner with one another. Database servers were established and all essential databases were mirrored between the on-premises datacenter and Azure. In case of failure in primary database, failover to Azure required manual initiation assisted by Azure Automation.

From a networking perspective, connectivity between the Land Register on-premises site infrastructure and the secondary site within Microsoft Azure was provided by a secure site-to-site virtual private network (VPN). The secondary Azure network infrastructure consisted of two separate subnets to divide the Land Register servers by function (application front-end servers and database servers). This facilitates the use of subnet based Azure Network Security Group (NSG) Access Control List (ACL) rules that allow or deny network traffic between systems residing in these tiers. Application health monitoring and application availability were handled by a hosted network appliance infrastructure, which employed health probes for both the on-premises and Azure infrastructures. In the event that the on-premises application servers do not respond, the network appliance assumes the primary site is down and forwards end-user requests to the Land Register front-end application servers hosted in Azure.

A conceptual diagram of the redundant components of the Land Register solution hosted in Azure are provided below for reference:

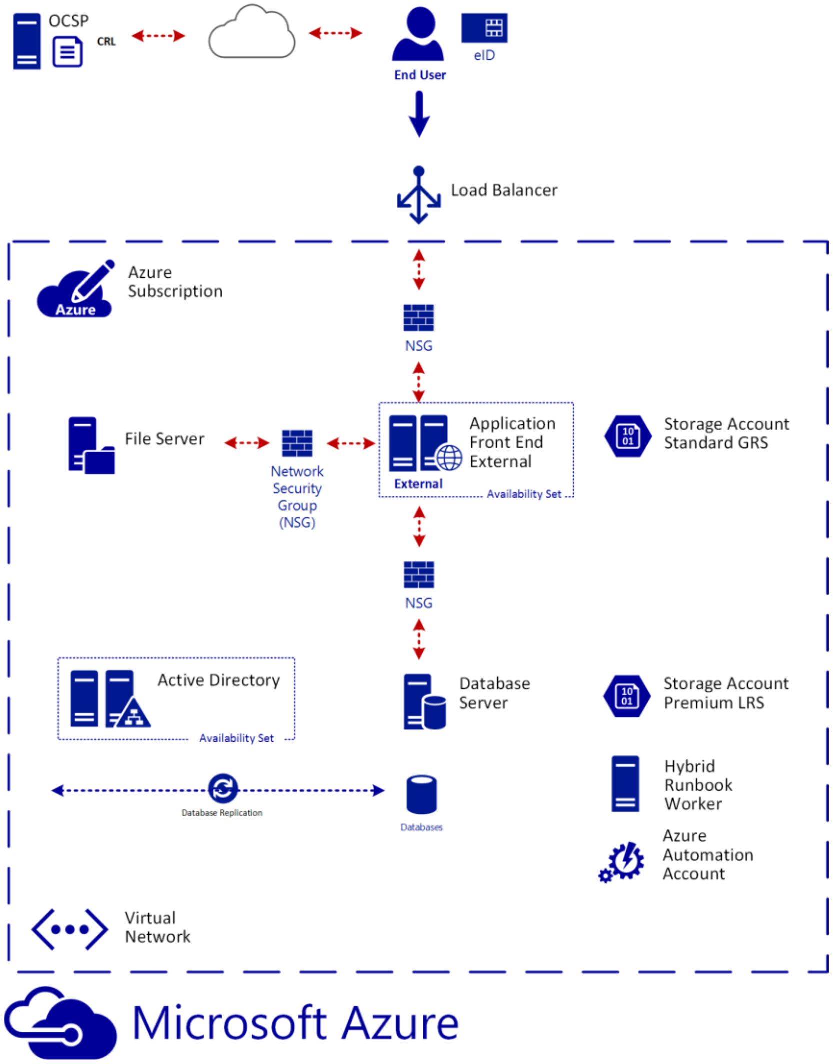


Figure 2: *Proof-of-concept public cloud application conceptual architecture*

8 Hypotheses for cloud enabled digital continuity

Following the approach taken during Phase I, a number of policy and technical hypotheses were developed for this new phase of the Estonia-Microsoft joint project. These Phase II hypotheses build on the lessons learned in the previous phase, and were tested by examining the feasibility of a critical Estonian government service using public cloud for resilience in the event of a crisis.

#	Hypotheses to be tested	Focus
1	Government services that fail over to the public cloud are able to continue to perform their essential functions.	Technical
2	Minimal application architectural changes required to the application to support failover to the public cloud of government services.	Technical
3	Existing platform architectures originally developed to run on-premises may require optimization to support public cloud platforms.	Technical
4	Acceptable recovery time objectives are achieved during recovery of the application services after failover.	Technical
5	Modification of on-premises failover and fail-back operational procedures will be required for digital continuity.	Technical
6	Government security standards and policy frameworks may need to be updated to enhance digital continuity for government services and public cloud use.	Policy
7	Implementing automated failover to the public cloud for governmental services is feasible.	Technical
8	There is a "trust gap" around public cloud in terms of security and transparency that can be best addressed between cloud providers and government.	Policy

Table 2: *Phase II Hypotheses*

The next few pages address each of these hypotheses on the basis of the lessons learned by the Estonia and Microsoft team in developing and discussing the proof-of-concept Land Register application.

9 Tested hypotheses

9.1 Hypothesis 1

Government services that fail over to the public cloud are able to continue to perform their essential functions

The testing of the Land Register as part of the research project, focused on failover in *forecasted* and *un-forecasted* disruptions. A *forecasted* disruption has foreseen impacts and can be mitigated with planned solutions. *Unforecasted* events have no mitigation plan in place, either due to the disruptions' immediacy or excessive impact from previously acceptable risk factors. Both types of disruption were addressed via redundant infrastructure in the form of Microsoft Azure virtual machines and Azure Automation.[10] The Land Register's various components and functions were tested for both scenarios, in Azure. All test cases were successfully executed and critical functions were found to operate without issue.

A key observation was the level of redundant public cloud infrastructure required for established, on-premises applications' failover. The initial Land Register public cloud design established full redundancy for each application tier (web, database) via multiple Azure virtual machines, in order to protect against local failures *within* the public cloud *after* failover. However, analysis determined that the Land Register's level of current on-premises, cross-datacenter redundancy was so substantial that it only needed a subset of functionality in Azure to function in a crisis. Should the crisis persist, more public cloud infrastructure can be added until the on-premises environment is stabilized. This reduced the application's footprint within Azure to core functions, balancing cost with redundancy while still supporting the failover goals.

Another observation relates to the applications and services which the Land Register depends upon. Due to the on-premises datacenter network connectivity to Azure, the application was still able to connect to necessary on-premises systems during failover, including DigiDoc services (for digital signing), the Estonian electronic identification system (eID), the Building Register and the Population Register. In a true crisis scenario, however, such services might also be affected and a public cloud presence or coordinated failover would be needed to ensure the application had full functionality. A service requiring failover should, therefore, have a Technical Dependency Analysis (TDA) to map service dependencies.

9.2 Hypothesis 2

Minimal application architectural changes required to the application to support failover to the public cloud of government services

A fundamental question in failover planning for the Land Register application was to understand what code-level changes might be required to each application to support public cloud redundancy. In some cases, application developers take programmatic dependencies upon the underlying datacenter infrastructure where they reside, e.g., "hard-coding" the application to the infrastructure. Code changes

[10] https://azure.microsoft.com/en-us/services/automation

are typically expensive to resolve. This can present challenges for applications to natively support portability across multiple physical datacenters during failover operations, including public cloud. Such inflexible infrastructure dependencies include binding to specific Internet protocol addresses, having dependencies on specific database servers, and having a dependency on a specific protocol or service which is not compatible with the target environment. In public cloud failover scenarios, this is particularly important since not all services, protocols or capabilities found within on-premises infrastructures are either present or have the same level of functionality in the public cloud.

In the case of the Land Register, the application did not have any hard dependencies to the on-premises infrastructure, making it a viable candidate for failover to multiple on-premises and public cloud hosting locations. The only required configuration changes were limited to modifications of application configuration files, supporting automation, and minor changes to the Land Register platform architecture in Microsoft Azure.

9.3 Hypothesis 3

Existing platform architectures originally developed to run on-premises may require optimization to support public cloud platforms

Unlike Hypothesis 2, which focused on code changes within the Land Register *application*, Hypothesis 3 focuses on changes required to the *platform*. While application-level changes refer to programmatic changes to the code of an application, platform-configuration changes are those which involve modifications to the systems the application runs upon. For example, platform changes may involve operating system-level changes such as deployment of different types of systems, storage or re-architecture of availability constructs. In this case, an expected observation was that many architectural aspects of the *cloud platform* that the Land Register runs on required optimization to support failover to the public cloud, primarily because not all on-premises constructs are available in the public cloud. No code-level changes were required to the Land Register application for this modification. The required optimization to the Land Register's use of the cloud platform included (operating system) upgrades, virtual machine size alignment with Azure offerings, and changes to the database architecture to support an application-level availability model.

Most public cloud services necessitate the use of supported operating systems, processor architectures and defined virtual machine sizes. These constraints support rigid standardization models that enable standard offerings for customers at hyper-scale. Conversely, on-premises infrastructures have a high degree of flexibility in each of these areas which application developers and systems administrators use to provide a given service. Any transition or extension into the public cloud must carefully consider what constraints this places on the application or service.

For the Land Register application, the adoption of Microsoft Azure virtual machine sizes and updated operating system versions were required to support public cloud failover. Additionally, some on-premises platform availability models, not currently supported in public cloud environments, required replacement by application-level availability models, in this case including transition from a SQL Server Failover Cluster to an SQL Always-On Availability Group high-availability model within the public cloud.

What became clear as consequence of testing this hypothesis is that, in general terms, a one-to-one transition model is not always possible when choosing public cloud to provide resiliency solutions and that minor levels of additional investment may be required.

9.4 Hypothesis 4

Acceptable Recovery Time Objectives achieved in recovery of application services after failover

Any continuity solution must meet the application's required Recovery Time Objective (RTO). RTO is the maximum time required from service disruption to restoration of the application's functions, including its data from a set recovery point. The ability to achieve this is referred to as Recovery Time Capability (RTC). For the Land Register proof-of-concept, the ability to failover to an instance residing in the public cloud within acceptable RTOs was enabled through three primary efforts:

1. Ensuring a replica of the web application codebase was deployed to systems hosted in both the on-premises and public cloud environments;
2. Ensuring regular, asynchronous replication of the data tier of the application was performed between the primary and secondary environments; and,
3. Developing supporting automation to trigger planned and unplanned failover between the on-premises and public cloud versions of the application.

The Land Register's Service Level Agreement (SLA) states that for planned failover the RTO is two hours, while the unplanned RTO is eight hours, with just 48 hours per year for planned interruptions and 96 hours per year for unplanned interruptions. During testing these objectives were met by the public cloud provider (Microsoft Azure).

The key observation for the joint-project team was that acceptable RTOs could be met via public cloud only if the systems and required dependencies for this exist within the public cloud prior to the failover event. If an essential element of an application needs re-deployment at time of failover, this must be planned for as part of a digital continuity strategy.

9.5 Hypothesis 5

Modification of on-premises failover and fail-back operational procedures will be required for digital continuity

During the proof-of-concept design it was assumed that some level of modification to the current continuity operational procedures would be required, in order to provide proper failover of the workload to the public cloud. Two areas of modifications were required to support failover:

1. Modification of the SQL Server infrastructure to support failover to SQL Servers running within Microsoft Azure (public cloud) virtual machines.
2. Development of automation to support planned and unplanned failover between the on-premises and public cloud instances of the Land Register application.

While these were minor changes, it should never be assumed that applications can use public cloud for resiliency without some level of change (and associated investment). Currently the systems which reside between two datacenters require manual switching of the data tier (SQL servers) while all other failover operations are automated. As part of the proof-of-concept, the failover process was regularly tested and improved.

9.6 Hypothesis 6

Government security standards and policy frameworks may need to be updated to enhance digital continuity and to address public cloud use

Governments have established policy frameworks and security standards that govern the use of ICT resources. However, rapid technological advances mean these frameworks must continue to adapt. As a consequence, public cloud use is often unaddressed by either policy, legislation, or public security standards. The research tested the hypothesis that governmental frameworks should be adapted, on the one hand, to explicitly set expectations for the cloud service provider, and on the other, to enable the use of public cloud.

Revisions to existing frameworks might include laws relating to data protection, data classification, and even government resilience, to ensure clarity as to when cloud computing should be appropriately considered and deployed. Expectations for cloud service providers could cover security certification and policies, proof of solvency, local customer support, etc., which a state would deem necessary as essential elements of trust.

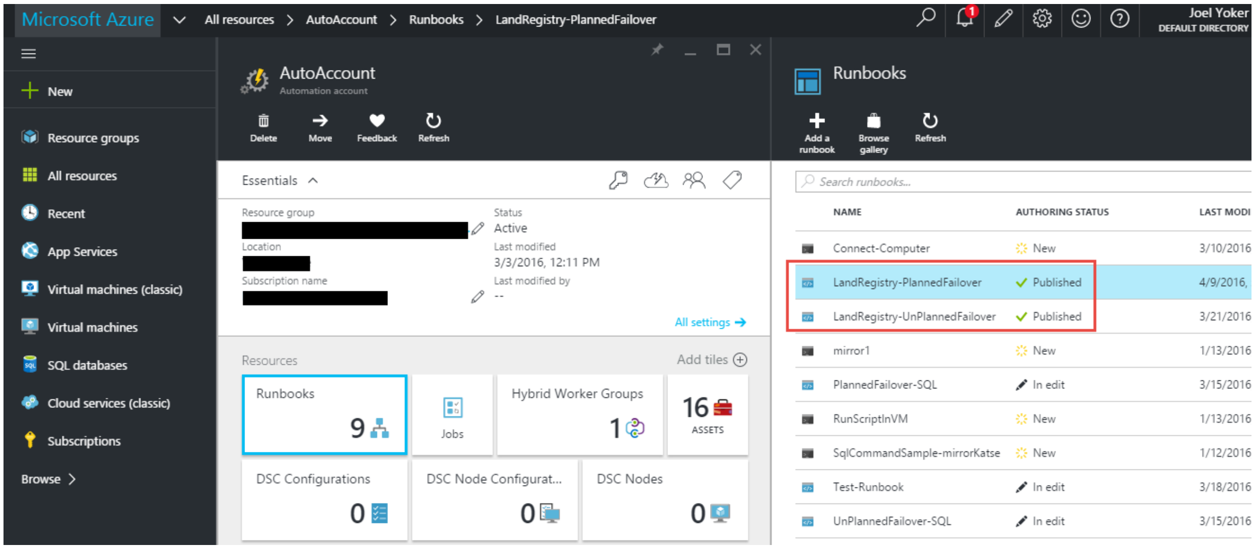
Governments may rely on one specific security standard, which only it might use. By asking public cloud service providers to comply with this one standard the state narrows its options for a partner. Compliance costs for a private-sector service provider to meet this standard could be economically unviable, especially for a small local market. At the same time, changing a country’s security standards would cost government, public bodies and already compliant companies. A compromise scenario, wherein states increase flexibility around security standards, while service providers comply with additional, commercially reasonable standards, could emerge in time.

9.7 Hypothesis 7

Implementing automated failover to the public cloud for governmental services is feasible

In on-premises workloads, the automated aspects of the failover and failback procedures typically reside within the primary and/or secondary locations where the workload resides. With public cloud resiliency, a third option exists where the failover automation can be hosted in the public cloud. This option was used in the Phase II proof-of-concept deployment, using Azure Automation to host the revised automation required to support cloud resiliency for the application. As outlined earlier, Azure Automation provides a cloud-based automation repository and platform which Land Register used to support failover automation. In scenarios where the on-premises infrastructure was inaccessible due to disaster or system failure, Azure Automation would provide a decentralized mechanism to orchestrate failover.

To support the connection between on-premises and public cloud hosted infrastructures, an Azure Hybrid Runbook Worker was deployed, as illustrated below:



Resource group
[redacted]

Location
[redacted]

Subscription name
[redacted]

Status
Active

Last modified
3/3/2016, 12:11 PM

Last modified by
--

NAME	AUTHORING STATUS	LAST MODI
Connect-Computer	New	3/10/2016
LandRegistry-PlannedFailover	✓ Published	4/9/2016,
LandRegistry-UnPlannedFailover	✓ Published	3/21/2016
mirror1	New	1/13/2016
PlannedFailover-SQL	In edit	3/15/2016
RunScriptInVM	New	1/13/2016
SqlCommandSample-mirrorKatse	New	1/12/2016
Test-Runbook	In edit	3/18/2016
UnPlannedFailover-SQL	In edit	3/15/2016

Figure 3: *Land Register Azure Automation infrastructure*

Initially, the Land Register application could not centrally support failover to the public cloud. This required an investment of time and development resources to design and implement a failover solution. Given the nature of the proof-of-concept infrastructure, the design of the automated failover solution leveraged native capabilities within the operating system and data platform for each failover scenario. This reduced the time needed to establish the capability. However, more complex scenarios or infrastructures would require a greater investment to modify advanced failover tasks. Organizations which choose public cloud resiliency capabilities should be prepared to invest in both automation and infrastructure to support their applications' standard failover and fail-back operations.

9.8 Hypothesis 8

There is a "trust gap" around public cloud in terms of security and transparency that are best addressed between cloud providers and government

Governments have a responsibility to pursue digital continuity in a way that meets public expectations of security and privacy. The foundation of a strong e-society is built on public trust. The same principle applies to an e-society where citizens can be certain that the government takes appropriate measures to protect their data. The stakes for governments which have adopted digital technologies, including public cloud, are much higher than just the data concerned: any breach of trust could damage society as a whole. Governments are particularly concerned about jurisdictional problems in relation to protecting people's data. Any agreement between a government and cloud service provider will need to address "trust gap" concerns specific to governments, including data integrity, access to data, data retention, and incident reporting.

Documentation, along with evidence of compliance, is only one part of assurance. Government processes that allow for acceptance of third party audits, which are supported by artifacts that demonstrate the efficacy of security capabilities that vendors have in place, can also help bridge the trust gap. In addition, governments should actively participate with standards organizations to define security and compliance standards for the cloud computing industry.

From a policy perspective, ongoing, open discussions around issues are needed to make up "trust gaps" such as government and law enforcement access to data that transits through or is stored in foreign countries. Discussion is also needed about the positive role of tools like transparency reports that cloud service providers use to create more awareness and transparency in how they handle customer data and respond to government requests to access that data. Additionally, a trusted relationship could be fostered if cloud service providers made relevant incident reports available to customers.[11] The EU's Network and Information Security Directive may also provide a framework for incident reporting for cloud service providers in Europe which is intended to enhance communication and trust between government and cloud service providers. Also, cloud service providers should share relevant information about law enforcement data access requests for information stored in the cloud. Microsoft, for example provides detailed data twice a year in a publicly available report.

From a policy and technical perspective, issues concerning data integrity of digital services are also an important long-term concern, going well beyond the scope of this report. Government and cloud providers will need to work together to ensure that there are appropriate mechanisms and artifacts to provide data integrity assurance that citizens, businesses and politicians may require.

Government and the private sector should also continue to explore more aspects of digital continuity, including data integrity. Specifically, efforts could be undertaken to address authorities which depend on a single source of trust, include root certificates, time stamping, and Domain Name Services that could benefit from distributed mechanisms of "proof of validity and integrity" for each digital record and transaction.

[11] Microsoft periodically publishes a Security Intelligence Report, along with regional threat assessments. See also Microsoft's whitepaper on *Azure Security Response in the cloud*, published April 11, 2016.

10 Findings and recommendations

10.1 Technical findings

Phase II's proof-of-concept can be seen as largely successful. The research dealt with read-only components of the Land Register and Online Certificate Status Protocol (OCSP) applications due to various limitations. This enabled the testing of the Land Register application's primary functions (including search and land property lookup); functionality around insert, change or deletion was not performed. Similarly, this restriction was placed on the OCSP service where valid eIDs were available but it was not possible to add, cancel or pause these eIDs.

The summary of the technical findings is outlined below:

1. ***Digital signing and certificate services in the public cloud***: Estonian government applications leverage an internally-managed OCSP infrastructure to check certificate revocation and to authenticate users against a hosted certificate revocation list (CRL). Moving this service to the public cloud did not deliver the expected results and was therefore not included in the proof-of-concept. This was due to the following reasons:
   - The Estonian OCSP infrastructure within the public cloud was not configured to use the public cloud OCSP infrastructure and the ID-card certificate contained a specific location of certificate revocation list (CRL).
   - Digital signing within Land Register and other governmental information systems are dependent on a digital signing service provided by the Estonian Certification Center. In cases where this service is inaccessible, digital signing functionality would fail making some application functions unavailable. Resolution requires additional investigation and development on the current digital signing solution to accommodate public cloud environments.
2. ***Data platform configurations in public cloud environments:*** A key finding was that government applications targeted for public cloud should be baselined in production, prior to selecting a target virtual machine size and storage infrastructure. In addition, preserving data integrity between private and public cloud database infrastructures during unplanned disasters requires additional planning.
   - In the initial implementation the Azure virtual machines used for the Land Register database tier were configured conservatively. However, during normal operation the performance of data tier was found to be unacceptably slow. After analysis it was determined that the initial virtual machine size and storage infrastructure did not provide enough performance capabilities to the SQL Server infrastructure of Land Register. Once the virtual machine was resized to use a higher performing tier and an Azure Premium Storage Account (backed by Solid State Drive storage) was leveraged, application performance improved and was found to be within acceptable levels.
   - As part of the testing for scenarios where the primary SQL database server becomes inaccessible and data is transferred to its mirror in Azure, the Land Register team faced the challenge of preserving application data integrity. Given that the Land Register data store is the only source for land ownership in Estonia, there is no acceptable level of data loss for the application. The question of how could data integrity be assured when the primary SQL database server is lost remains to be answered. Similarly, we need to understand whether it is more acceptable to preserve data integrity or application functionality, if that choice needs to be made.

3. ***Public cloud network connectivity:*** As with most public cloud infrastructures, network connectivity to Microsoft Azure can be performed using a basic site-to-site Virtual Private Network (VPN) connection or through a dedicated peered connection, such as ExpressRoute.[12] As part of the research, challenges were encountered relating to connectivity to the public cloud. However, they were eventually resolved. The following observations were made:

   - Data upload speeds to Azure over a basic site-to-site VPN connection were initially found to be unusably slow for full-scale operations for Land Register. In some cases, initial speeds of 300-400 Kbps over the VPN solution were observed and it was determined that these conditions would not support keeping the Land Register database synchronized. The root cause was determined to be that the VPN device was not on the list of Azure validated VPN devices and was contributing to Internet Key Exchange negotiation errors. Upon switching to a validated VPN device, the network speeds between on-premises and Azure improved with file copies occurring within acceptable thresholds.
   - Due to the use of non-standard Microsoft support channels, resolving this issue took more time than expected and in a production setting it would have been unacceptable. For the production settings a suitable support agreement with contractual Service Level Agreements (SLA) should be established prior to production deployment of a public cloud failover solution.
   - In some cases, network appliance licenses used on-premises may not be supported by public cloud virtual appliances. In the Land Register application infrastructure, the Brocade virtual appliance was temporarily replaced to overcome this licensing issue.

4. ***Public cloud network configurations.*** In public cloud environments TCP/IP addresses are issued to virtual machines dynamically, which means that when these systems are deallocated from Microsoft Azure their associated virtual IP addresses can change. This presented some during normal operations and maintenance of the Land Register application.

   - When Microsoft Azure virtual machines are running they preserve their Virtual IP address, however when in a stopped and deallocated state, the assigned TCP/IP addresses (public and internal) are released to the pool. This creates a situation for systems and load balancers which are configured to access systems by a specific TCP/IP address. To overcome this problem, Microsoft Azure supports the ability to reserve TCP/IP addresses for both systems and their public interfaces. During the proof-of-concept this was a required step and it caused minor delays in implementation due to the loss of TCP/IP address assignment during routine maintenance.
   - It is recommended that for tiers of an application which require static TCP/IP address assignment (such as interfaces for external load balancers and domain controllers), these should be reserved during initial implementation.

5. ***Public cloud resiliency requires advanced planning and deployment to be effective.*** During the proof-of-concept it was noted that acceptable RTOs could be met with a resiliency strategy that uses public cloud, however this was only possible due to the pre-planning and deployment of services in the public cloud in advance to the failure event. The ability to meet RTOs depends heavily on whether or not the systems and all required dependencies exist within the public cloud prior to the failover event. If any essential element of the application requires re-deployment at time of failover, the RTO would be adversely impacted. In those cases, the ability to satisfy availability expectations would face significant challenges and should be considered when developing a public cloud resiliency strategy.

[12] https://azure.microsoft.com/en-us/services/expressroute

10.2 Policy recommendations

In order to enhance digital continuity for government services, states of all sizes should consider the use of cloud, including taking the following actions:

1. ***Include a digital continuity principle.*** An essential starting point for digital continuity policies and procedures would be addressing how failover of prioritized government services to the cloud should be managed. Based on this, each relevant government institution could then continue to develop its digital continuity capability to ensure resilience for its services.
2. ***Conduct a thorough risk assessment for each class of data and service if a migration to public cloud is considered.*** Once government agencies have classified their data and services based on their risk profiles, they should conduct a risk assessment. This assessment should include, among other things:
   - The risks associated with replicating data and services in the cloud for disaster recovery purposes;
   - How important it would be for users to be able to access data or services quickly in the event of a disruption or national disaster; and,
   - Whether the government's existing ICT infrastructure is able to ensure the necessary resilience and availability in the event of a disruption or disaster.
3. ***Establish a prioritized list of government services for digital continuity.*** As part of this prioritization, governments could consider formally listing e-services or databases that are "critical" to the functioning of the government and which society is reliant on. For example Estonia's Land Register contains crucial information linked to property ownership for which there is no paper backup. This "critical service" perspective often incorporates a wider selection of services than those probably already identified by governments as "vital services," upon which life and well-being depend. Such critical services would certainly include information systems like the Land Register or State Gazette, where unavailability for any significant period of time would be unacceptable. After a thorough risk assessment, some of these services might be considered appropriate for public cloud use.
4. ***Update public policies and principles, as needed, to enable appropriate use of public cloud for prioritized government services under certain circumstances.*** Pre-Internet, pre-online policies may inadvertently erect barriers to cloud services. Governments must make sure that appropriate safeguards are in place, proportional to risks and avoiding the creation of unnecessary obstacles to cloud computing use.
5. ***The digital continuity governance process should be periodically reviewed.*** As technology continues to evolve, policies and procedures must be re-evaluated to adapt and support pragmatic use of such technologies.
6. ***Government and private sector need to work together to help bridge the "trust gap"*** including adapting international standards to better address how vendors manage security in their software and operations, as well as ensuring appropriate artifacts that demonstrate the efficacy of security capabilities that vendors have in place.

11 Research project team

Executive Sponsors

Taavi Kotka, CIO, Ministry of Economic Affairs & Communications for Estonia

Mehis Sihvart, Director, Center of Registers and Information Systems

Anand Eswaran, Corporate Vice President, Microsoft Services

Rain Laane, Estonia Country Manager, Microsoft

Technical Project Leads

Mikk Lellsaar, Ministry of Economic Affairs & Communications for Estonia

Joel Yoker, Microsoft Services

Bruce Johnson, Microsoft Services

Policy Project Leads

Karoliina Ainge, Ministry of Economic Affairs & Communications for Estonia

Laura Kask, Ministry of Economic Affairs & Communications for Estonia

Tyson Storch, Microsoft Services

Contributors

Tomaz Cebul, Microsoft Services

Kaja Ciglic, Microsoft CELA

Lewis Curtis, Microsoft Services Disaster Response

Dejan Cvetkovic, Microsoft Regional Technology Officer

Kaur Kullman, Estonia State Information System Authority

Tiit Leppikus, Estonia Centre of Registers and Information Systems

Rome Mitt, Centre of Registers and Information Systems

Theo Moore, APCO Worldwide

Hallar Mölder, Tallinn University of Technology

Ian Nelson, Microsoft Services

Paul Nicholas, Microsoft CELA

Rebecca Radloff, Microsoft CELA

Junior Sawney, Microsoft Services