Cloud Adoption Policy Addendum

Trent Broderick

University of Maryland Global Campus

October 27, 2020

**Executive Summary**

This document is meant for the use of the executive team of BallotOnline to better prepare our policies on Cloud Migration. This addendum is meant to be used in conjunction with current Cloud Adoption Policy to further strengthen and improve our stance on BallotOnlines cloud migration needs. Covered by this document are improvements to the current Cloud Adoption Policy, our growth projections, service level agreement needs, security strategies pertaining to applications and data as well as and exit strategy plans for contingency of BallotOnline services.

It is asked that the leadership team reads this addendum with urgency as this addendum is mission critical to moving critical BallotOnline applications into the cloud. Without the implementation of these addendums, BallotOnline is positioning itself to take on more risk than what is considered reasonable. This document specifically mentions every scenario in our current cloud adoption policy that could lead to additional risk and or, negative business implications and how BallotOnline can update is policy to avoid said risk.

**Policy Scope**

**Overview**

This policy is to ensure both BallotOnline has a more specific understanding of the needs that need to be addressed buy the service-level agreement (SLA), the cloud adoption policy, and other related strategies and agreements. This addendum is to better fit the SLA policies and cloud adoption policies to the real-world needs of BallotOnline, our applications and data security. Due to the nature of BallotOnline and its business model, there are additional considerations for downtime, response, security and overall experience. Each “Cloud Ready” application will be leveraged against the current cloud adoption terms and SLAs to ensure the full support BallotOnline needs to operate is met by the chosen cloud service provider.

**List of Approved "Cloud Ready" Applications**

The following are cloud ready applications with considerations for the type of cloud service that would be most suitable. The BallotOnline email system, which is best kept in a SaaS style of cloud ownership as BallotOnline does not need any advanced control over the system, Ofice365 or G-Suite is preferred.

The DevOps CI/CD Pipeline, and additional development tools should be utilized in a PaaS fashion. Leveraging tools like Jenkins or TravisCI is a preferred motion by the DevOps team and would like to have some opinion in what tools they can use when developing for BallotOnline.

For the Backup and Archiving use case, BallotOnline resources and IaaS solution so the backups can be archived in multiple clouds in multiple availability zones in to protect against any type of single source failure.

**Alignment with Existing IT policies**

This addendum is not meant to fully replace current and existing IT policies. This addendum is meant to be used in conjunction with current policies and strengthen and or, better define current policies to further explain BallotOnlines needs and or strategy. The following existing policies are be amended for further improvements to BallotOnline: Service-Level Agreements in the Cloud, Data Security, Privacy, Governance, Cloud Vendor Governance and Exit Strategy.

In addition to addendums to current policies, also included for the use of BallotOnline executives in understanding the pace of BallotOnline IT usage and infrastructure is a Growth Projections Analysis, Business and Technical Impacts as well as definitive resources for escalation and policy conduct investigation.

**Growth Projections Analysis**

Table

Description automatically generatedTo the left is Figure 1, a historical trend of how BallotOnline has grown since 2012/13. During this time, we have seen a year over year growth in users from 2012 – 2017 at 180%, an average growth of 36% per year. Based on current market trends, we are estimating an average of 10% growth per year for the next three years. By the end of 2020, we are estimating approximately 2,000,000 users. By end of 2023, we are estimating a possible total number of users to reach 2,662,000 users. As of 2016/17 we estimated that per server we can handle 1,364 users, per switch we can handle 50,000 users, and each user uses about 1.67 gigabytes of data.

Figure 1 (UMGC,2020)

Using the estimates above, based on an estimate of 2,662,000 users, we will need 1,952 servers (an increase of 588 servers in total or 196 servers per year), 54 switches (an increase of 14 in total or 4/5 per year), and 4.45 pbs of storage (an increase of 1.95 pb in total or .65 pb per month). Based on these numbers alone, it is best for BallotOnline to looks for a large cloud service provider that at has available inventory in case we meet or exceed our growth projections.

The projections above do not consider the potential impact of Covid-19 on BallotOnlines user base. As it has been noticed, voting is at an all-time high amid this pandemic, so we are not anticipating any true loss of users through the 2020/2021 fiscal year. However, due to fluctuations in government spending, we cannot predict if the uptick in voting will have any major increase in users to our platform as governments may not be looking to invest in online voting platforms and instead my reinvest in themselves to stay afloat.

**Service-Level Agreements in the Cloud**

There are additional considerations we must make for “Cloud Ready” applications and the Service-Level Agreements pertaining to them. In this section, the RTOs, RPOs, Disaster Recovery and Back Up requirements, acceptable outage impacts, acceptable latency, geographic availability and any other gaps in the SLAs. Acceptable security requirements are considered in the Data Security portion of this document.

**Recovery Time Objectives and Recovery Point Objectives for Cloud Ready Applications**

Regarding Recovery Time Objectives, the acceptable amount of time a service is interrupted, acceptable terms per application are dependent on the application itself. For email, the acceptable RTO is 15 minutes. For backups and archiving, the acceptable RTO is 30 minutes. For software development, there is no acceptable RTO, as a matter of fact, all software development applications must be always accessible and always available.

For the Recovery Point Objective, the amount of time since the last recovery point, the acceptable amount of time also varies from application to application. For email, the acceptable amount of time is 0, email must be always accessible for BallotOnline. For software development, the acceptable RPO is 15 minutes. For backups and archiving, the acceptable RPO is 30 minutes.

**Disaster Recovery and Backup Requirements**

BallotOnline also needs additional added addendums to policies regarding disaster recovery and back ups outside of RTOs and RPOs. It is required that BallotOnline is billed monthly with at least one petabyte of storage available to store back up data too. The disaster recovery cloud infrastructure may be owned by a separate cloud service provider to ensure during disaster recovery there are no infrastructure related single point failures. It is best practice that all back up infrastructure is available to be spun up and activated within 15 minutes.

**Impacts of Outage**

The above policies are meant to mitigate the impact of an outage. An outage can impact more than just services as it can impact the BallotOnline brand, its customer relationships, loss of revenue, SLA violations and employee workflows. The goal of outage mitigation is to ensure all employees, customers and stakeholders in BallotOnline remain confident in the processes and professionality of BallotOnline in case of an outage.

**Acceptable Performance Standards and Geographic Availability**

For application performance, it is asked that BallotOnline measure acceptable latency and IOPS for its applications. Latency refers to the time between user action and reaction; while IOPS refers to the read and write capabilities of storage appliance connected to the infrastructure. BallotOnline. Must test each application to understand the main metrics, the lowest possible IOPS and highest possible Latency, the optimal IOPS and latency, and the highest IOPS and lowest possible latency the applications can tolerate. This will help with competitive pricing across multiple cloud service providers.

The cloud service provider must provide a high available cloud architecture that allows data to say geographically integral. US data should not leave the US while EU resident data cannot under any circumstances leave the EU. All data regulations must follow the best practices as outlined by the respective counties data privacy laws and the GDPR.

**Data Security, Privacy, and Governance**

**Network Security Design and Issues**

Network security relates to all policy and procedures that can help mitigate risks from a network standpoint (UMGC, 2020). It is key that BallotOnline systems are placed in pure Layer 2 with absolutely no access to the public internet. Furthermore, all systems must be interconnected using dark fiber to ensure further security across the devices. Only approved routers, routing appliances, vxLans, and firewalls provided by the cloud service provider can be used in this architecture. IP Tables and ports are to be configured via scripting and manually reviewed whenever possible to ensure full networking topological security. In order to address security issues there are several steps that need to be taken to avoid and simple security issues, these steps include, policies regarding datacenter security (SOC-2 Type-2 attestation preferred), previously mentioned policies regarding network security, Account Access policies regarding IAM roles or SSH key roles, properly architected applications and software built to be resistant to virus and malware attacks, and policies regarding data security.

**Data Security and Compliance**

Leveraging the CIA Triad (UMGC, 2020), which takes in confidentiality, availability and integrity is a best practice when it comes to information security. Confidentiality leverages methods to protect privileged information from unauthorized disclosure. BallotOnline process several sensitive records daily that could impact elections, and the people who vote in them. Integrity refers to the processes that ensure that data is correct, accurate and unchanged. It is extremely important to the brand of BallotOnline that customer information or voting remains integral and safe of editing, spoofing or destruction. Availability refers to the system and its data being readily accessible in case of any kind of failure. In the section regarding Cloud Ready SLAs, the needs for availability were addressed.

For compliance, data is classified in multiple ways. It is critical for BallotOnline to continue to develop policies that focus on the security of data at rest (on the physical disk), data in use (active in the RAM or CPU), data in transit, classifying the information and data properly as well as the ability to move and or lock down certain data either for security or compliance reasons such as GDPR (UMGC, 2020). It is preferred that data is stored in single tenant environments and that the providers datacenter is accurately listed to ensure data is being properly stored. Furthermore, all cloud vendors must meet the same regulatory procedures that BallotOnline must also comply to (UMGC, 2020). The main framework to be leveraged when considering compliance issues is IRAC (Issue, Rule, Application, and Conclusion).

**Cloud Vendor Governance Strategy**

In order to properly assess a cloud vendor, a cloud vendor governance strategy must be put in place. This strategy must include the rules of engagement with cloud vendors, the procedures and security compliances must match the needs of BallotOnline and the assessment from a third party is suggested but not required. While price is important, the cloud vendor must be able to provide minimally the following to BallotOnline; single tenant systems, advanced networking and network security protocols in a managed service, a disaster recovery environment that still allows data to remain geographically compliant, data protection, data integrity geographically, and available inventory for burstable workloads when needed. It is best that the cloud vendor can meet all the terms in our existing SLA as well as any additional security compliances found to be paramount to the business of BallotOnline.

During engagement, BallotOnline must evaluate minimally two different providers and should consult with a third part for non-biased results. All calls and interactions with cloud vendors are to be recorded and noted to ensure a clear path from start to finish for further integrity. It is best practice to choose a solution that not only fits the business needs both for infrastructure and security but is cost effective and BallotOnline only pays for services it uses.

**Business and Technical Impact**

Moving to the cloud with have a tremendous impact on how BallotOnline approaches the market and positions itself to do business at the edge. On the business end, the possibilities are truly endless. BallotOnline now has the ability to place servers in new markets at a moment's notice. In traditional colocation or internal datacenter management, this process of breaking into a new market could take between six weeks and six months, in the cloud, a server can be spun up in six minutes. This means BallotOnline can not only market test faster but operate servers in a CAPEX model that allows BallotOnline to recognize new lines of revenue much faster. Cloud vendors are not only at the edge, but also highly available at the edge. While BallotOnline focused mainly on the US and EU markets, now not only is able to expand in these markets but also reach Asia and Australia, but also the Baltics, Mediterranean, Middle East and India.

On a technical standpoint, BallotOnline takes the step into the future with this digital transformation. Instead of relying on hardware that starts to depreciate immediately and is often needed to be updated every three to five years, in the cloud BallotOnline can receive the newest and best servers on the market. This may allow BallotOnline to consolidate and shrink its footprint with high performant servers. Furthermore, BallotOnline has access to a growing ecosystem of ready for cloud services that can integrate well with in the DevOps and So9ftware Development ecosystem. No longer will BallotOnline need to employ hundreds of people to manage the hardware as the cloud vendor takes on the responsibility. BallotOnline can now use this additional revenue to reinvest into itself.

**Exit Strategy**

There are several scenarios when BallotOnline must consider exiting from its relationship with a cloud vendor. Some of these scenarios include multiple SLA violations, price gouging, lack of support, multiple outages and similar issues. In the event an exit strategy is considered, instead of moving out of the cloud, BallotOnline will consider three new cloud vendors that meet the needs of BallotOnline for both cost effectiveness, security and data compliances. It is recommended BallotOnline do not leverage cloud vendors proprietary managed services as they can be difficult to migrate off of.

**Resources and Escalation Contacts**

For additional resources, please leverage internal docs posted in the INFOSEC Google Drive folder. In that folder will also be additional resources regard SDLA Violation escalation. Please reach out to the CISO, CEO, CTO or the Cloud Policy team for further questions.

**References**

UMGC. (2020a). *Application and Data Security*. Www.Umgc.Edu. https://leocontent.umgc.edu/content/umuc/tgs/cca/cca630/2208/learning-topic-list/application-and-data-security.html?ou=516113

UMGC. (2020b). *Cloud and Network Security Issues*. Www.Umgc.Edu. https://leocontent.umgc.edu/content/umuc/tgs/cca/cca630/2208/learning-topic-list/cloud-and-network-security-issues.html?ou=516113

UMGC. (2020c). *Cloud-Specific Compliance Issues*. Www.Umgc.Edu. https://leocontent.umgc.edu/content/umuc/tgs/cca/cca630/2208/learning-topic-list/cloud-specific-compliance-issues.html?ou=516113

UMGC. (2020d). *Data Compliance*. Www.Umgc.Edu. https://leocontent.umgc.edu/content/umuc/tgs/cca/cca630/2208/learning-topic-list/data-compliance.html?ou=516113

UMGC. (2020e). *Network Security Design*. Www.Umgc.Edu. https://leocontent.umgc.edu/content/umuc/tgs/cca/cca630/2208/learning-topic-list/network-security-design.html?ou=516113