BallotOnline Cloud Adoption: Risk, Compliance, and Data Governance Analysis

Kareem Rizk

University of Maryland Global Campus

DCL 600T 9042 Decisive Thinking, Communicating, and Leading in Technology Fields

Professor Oussama Saafein

May 19, 2025

Cloud Risk Concepts and Risk Factors

Cloud computing is rapidly transforming the way organizations operate, from small businesses to large enterprises and government institutions. As of 2025, over 94% of enterprises have adopted some form of cloud service, and nearly 70% of government entities globally report ongoing cloud migration initiatives (Statista, 2025). The flexibility, scalability, and cost-efficiency of cloud services have accelerated digital transformation across all sectors. However, this shift brings a set of inherent risks that must be carefully assessed before adoption. For a Software-as-a-Service (SaaS) company like BallotOnline, considering migration to an Infrastructure-as-a-Service (IaaS) model, understanding risk is essential.

This report provides a comprehensive analysis of the technical, legal, regulatory, and compliance risks associated with BallotOnline's planned transition to cloud infrastructure. Key areas examined include service-level agreements (SLAs), data privacy regulations such as GDPR and CCPA, security vulnerabilities, and U.S. legal system implications. A structured risk matrix was developed to categorize and prioritize these risks.

Based on the analysis, a high-level compliance program is proposed to mitigate these risks and ensure BallotOnline remains in compliance with applicable laws and industry-specific mandates, particularly in the elections sector. This summary and the accompanying recommendations are intended to guide BallotOnline's executive leadership in making informed, secure, and legally sound decisions throughout the cloud migration process.

Understanding Cloud Risk at the Organizational Level

may lead to loss of operational visibility and control. Key concerns include vendor insolvency, unexpected service termination, and incompatibility with regulatory requirements. Even with frameworks like FedRAMP, which standardizes security for cloud vendors working with U.S. federal agencies, residual risk remains with the client (UMGC, 2025b). Mitigation requires continuous monitoring, strong auditing, and well-defined memoranda of agreement (MOA).

SLAs (Service-Level Agreements) are meant to guarantee availability and support levels, but they don’t always ensure compensation in critical failures. If BallotOnline suffers downtime from its provider during an election event, it could face reputational and financial consequences despite minimal SLA remedies (UMGC, 2025c).

Real-World Case Studies

- A major incident involved AWS S3 buckets misconfigured to be publicly accessible, leading to sensitive data exposure (Cloud Security Journal, 2023).
- Another case revealed how lack of backup strategies caused permanent data loss (Data Risks in the Cloud, 2024).
- IAM misconfigurations have led to unauthorized access and elevated privileges being exploited (Dimensions of Security Threats, 2023).

These examples illustrate the critical need for strong identity governance, role-based access controls, and robust backup protocols.

Risk Assessment Framework

The NIST SP 800-39 risk management process includes:

- Frame – Identify assets, threats, vulnerabilities.
- Assess – Evaluate likelihood and impact.
- Respond – Choose among acceptance, avoidance, transfer, mitigation.
- Monitor – Continuously track risk environment (NIST, 2011).

For instance, BallotOnline might assess a “data breach from misconfigured storage” as a high-likelihood, high-impact risk, choosing mitigation via encryption and least-privilege access.

Risk Assessment Framework

Risk Factor	Description	Mitigation
Vulnerabilities	Unpatched systems	Patch management, scanning (UMGC, 2025d)
Endpoints	Device loss/theft	Encryption, remote wipe
Regulations	GDPR non-compliance	Compliance programs, audits (UMGC, 2025e)
Data overload	Poor data governance	Classification, data lifecycle policies

Identification of the Most Appropriate Guidelines for Managing Risks

1. **NIST Cybersecurity Framework:**

The NIST Cybersecurity Framework offers a voluntary, risk-based approach to managing cybersecurity (NIST, 2018). Developed through collaboration between public and private sectors, it aligns with organizational business needs without imposing regulatory burdens. For BallotOnline, NIST is particularly appropriate due to its role in the Help America Vote Act of 2002, which authorized NIST to provide technical guidance to the U.S. Election Assistance Commission on voting system security, fraud detection, and voter privacy (UMGC, 2025a).

2. **ISO Standards (ISO/IEC 27001 and ISO 31000):**

ISO/IEC 27001 provides a systematic framework for managing information security risks, while ISO 31000 outlines enterprise-wide risk management principles (UMGC, 2025b). These internationally accepted standards help organizations implement security policies, access control, incident response, and compliance frameworks. Their global recognition makes them ideal for BallotOnline's operations and scalability.

3. **FedRAMP:**

FedRAMP delivers a unified security authorization framework for cloud service providers working with federal agencies. It ensures compliance with U.S. government security standards and facilitates the reuse of authorizations across agencies (UMGC, 2025c). For BallotOnline, aligning with FedRAMP enhances its potential for public-sector engagements.

4. **Cloud Security Alliance (CSA):**

The Cloud Security Alliance provides practical, up-to-date best practices, certifications, and tools for cloud security, developed in collaboration with industry and government stakeholders. Its flexible and vendor-neutral guidelines help reinforce traditional compliance frameworks like NIST and ISO (CSA, n.d.).

Identify Potential Privacy Issues and Mitigation Measures

Cloud Security Alliance (CSA):

As BallotOnline expands globally, it must comply with a diverse set of international privacy regulations. The most critical among these is the European Union's General Data Protection Regulation (GDPR), which applies to any organization processing personal data of EU citizens, regardless of where the organization is located (Kottasová, 2018).

GDPR defines personal data broadly to include any information related to an identifiable person and mandates "privacy by default" in all data handling activities (European Commission, 2018). Given that BallotOnline handles highly sensitive voter information, the following GDPR principles are especially relevant: lawfulness and fairness, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.

BallotOnline must adopt technical and organizational controls that align with these principles. Specifically, data of EU citizens should be hosted exclusively in EU-based data centers, and access must be restricted to authorized personnel. Additionally, data transfers to non-EU regions should be blocked by default unless supported by EU-approved mechanisms, such as standard contractual clauses or reliance on providers like AWS with specific EU data transfer approvals (AWS, 2018).

Further, BallotOnline should appoint a Data Protection Officer (DPO), implement multi-factor authentication (MFA), and require explicit consent from users for data collection and processing. Regular employee training and security audits will reinforce compliance and minimize breach risk.

Failure to comply may result in regulatory fines up to €20 million or 4% of global annual turnover (IAPP, 2017). Therefore, aligning with GDPR not only ensures legal compliance but also enhances trust and credibility with European stakeholders.

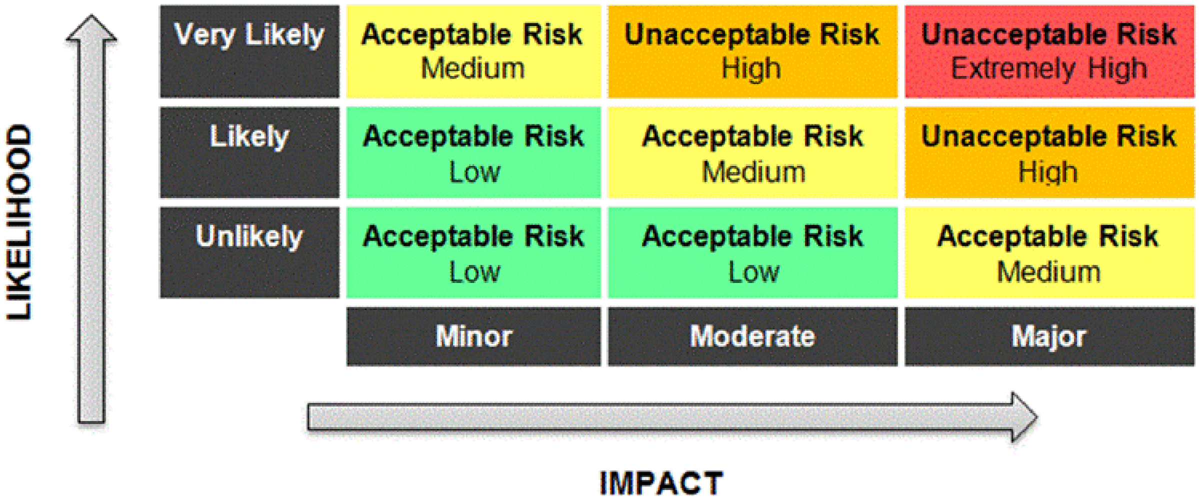
Risk Management Matrix and Analysis

Risk Management Matrix and Analysis

As part of BallotOnline’s cloud risk and compliance assessment, a Risk Management Matrix has been developed to evaluate and categorize potential risks based on their *likelihood of occurrence* and *impact severity*. This structured approach enables the organization to prioritize risk mitigation strategies and allocate resources effectively.

Understanding the Matrix

Figure 1: Standard Risk Matrix:



Very Likely	Acceptable Risk Medium	Unacceptable Risk High	Unacceptable Risk Extremely High
Likely	Acceptable Risk Low	Acceptable Risk Medium	Unacceptable Risk High
Unlikely	Acceptable Risk Low	Acceptable Risk Low	Acceptable Risk Medium
	Minor	Moderate	Major

LIKELIHOOD
IMPACT

Source: University of Maryland Global Campus (2025)

Risk Matrix Summary

The completed matrix covers six key risks relevant to BallotOnline’s cloud-based voting infrastructure. These include internal operational risks (e.g., data breaches, downtime, misconfigurations) and external threats (e.g., nation-state attacks). Each risk is evaluated based on probability, potential damage, and mitigation approach.

Risk ID	Risk Name	Likelihood	Impact	Risk Level	Mitigation Strategy

R1	Data Breach of Voter Information	Very Likely	Major	Extremely High	Encrypt data at rest and in transit, enable MFA, restrict access to authorized roles only
R2	Cloud Service Downtime (Election)	Likely	Major	High	Multi-region deployment, backup infrastructure, SLAs with cloud provider
R3	GDPR Non-Compliance	Likely	Moderate	Medium	Appoint DPO, audit data handling, store EU data in EU regions only
R4	Unauthorized Admin Access	Unlikely	Major	Medium	Implement RBAC, conduct regular access reviews, enable logging
R5	Data Loss due to Misconfiguration	Likely	Moderate	Medium	Use Infrastructure-as-Code (IaC), enforce version control, automated testing for deployments
R6	Nation-State Cyber Attack (e.g., Election Interference)	Unlikely	Major	High	Leverage threat intelligence services, enable IDS/IPS, geo-redundant backups, implement incident response plan

One of the most significant inclusions is the "Nation-State Cyber Attack" threat. Inspired by documented cases of political interference—such as the alleged Russian cyber operations targeting the 2016 U.S. presidential election (U.S. Senate, 2019)—this risk is categorized as high impact despite its relatively lower likelihood. Mitigating such risks requires proactive strategies like real-time intrusion detection, threat intelligence from the cloud provider, and geographically redundant backups.

For a full and properly formatted version of the risk matrix, see the accompanying spreadsheet BallotOnline_Risk_Management_Matrix.xlsx.

Cloud and Network Security Issues

BallotOnline’s cloud infrastructure introduces several key security challenges that must be addressed. Among the most critical are data in transit vulnerabilities, which expose sensitive election data to risks such as packet sniffing and spoofing. These can be mitigated through encryption protocols and intrusion detection systems (UMGC, 2025a). Endpoint and external storage vulnerabilities also pose threats, especially when users rely on personal or mobile devices, making endpoint protection and port controls essential.

Multifactor authentication (MFA) is required to secure administrative access by combining password, device, and biometric verification (UMGC, 2025b). Additionally, identity and access management (IAM) must enforce role-based access, least privilege, and periodic reviews to prevent privilege escalation (Chickowski, 2013).

To ensure data integrity and availability, BallotOnline should also secure its infrastructure using cloud-native tools for encryption, logging, and denial-of-service protection (NIST, 2010). Overall, a layered defense model combining technical controls and policy enforcement is essential to securing the platform.

US Legal System, Intellectual Property, and Cyberspace Law

BallotOnline, as a U.S.-based SaaS provider, must operate in compliance with both federal and state legal systems, particularly in the context of cloud computing. Most cloud-related legal matters fall under federal jurisdiction due to the interstate nature of internet communication, including issues related to data breaches, digital agreements, and intellectual property (UMGC, 2025a). Violations of cybersecurity laws may lead to both civil penalties and criminal charges, depending on the nature and scope of the incident.

Understanding the structure of the U.S. legal system is essential. It consists of legislative, executive, and judicial branches, each with distinct but interconnected roles. Legal cases may proceed through the court system or be resolved through alternative dispute resolution (ADR) mechanisms such as arbitration or mediation. Given the complexity of cyberspace law, cloud service agreements should include clear jurisdiction clauses and well-defined terms for resolving disputes.

In addition, intellectual property law is especially important for BallotOnline, which relies on proprietary software and digital assets. Copyright, trademark, and patent protections help guard against infringement, counterfeiting, and unauthorized use (UMGC, 2025b). To protect these assets, BallotOnline must enforce technical safeguards and legal controls.

Cyberspace law also governs key issues such as electronic contracting, digital signatures, intermediary liability, and data governance. Negotiating a cloud hosting agreement requires knowledge of legal terms such as service descriptions, performance standards, data deletion policies, liability clauses, and SLA enforcement. These agreements should also account for international users and data localization, ensuring compliance with both U.S. and foreign regulations (UMGC, 2025c).

By proactively addressing these legal and regulatory dimensions, BallotOnline can better manage risks, enforce intellectual property rights, and ensure operational integrity in a legally compliant cloud environment.

Applying a Compliance Analysis Framework

To structure the analysis of complex legal and compliance issues in cloud computing, the IRAC framework—Issue, Rule, Application, Conclusion—is selected as the most suitable approach for BallotOnline’s context. This method is widely taught in U.S. law schools and offers a straightforward and legally rigorous approach to issue analysis (University of Maryland Global Campus [UMGC], 2025). It is particularly effective in structuring assessments of cloud-related concerns such as data sovereignty, intermediary liability, or intellectual property violations.

By applying IRAC, BallotOnline can consistently evaluate each issue by identifying the legal question, referencing relevant statutes or principles (e.g., federal data protection laws), applying those rules to the organization’s operational reality, and drawing a clear, actionable conclusion. While ILAC and CREAC provide expanded variations with more explanation or flexibility, IRAC's clarity makes it ideal for legal compliance decisions in technical settings.

Legal and Compliance Issues – Industry, Geographic, Cloud, and Data Considerations

As a cloud-based elections technology provider, BallotOnline must comply with legal and regulatory frameworks that span across its industry, operational geography, and cloud infrastructure. These requirements are critical to maintaining lawful operations, protecting user data, and avoiding costly legal consequences.

Industry-Specific Compliance

BallotOnline must adhere to U.S. election laws, primarily the Help America Vote Act (HAVA) and the Federal Election Campaign Act (FECA). These laws regulate system security, integrity of voter data, and proper campaign data handling. Noncompliance could result in legal sanctions and reputational harm (UMGC, 2025a).

Geographic Compliance

Operating internationally, BallotOnline is subject to the General Data Protection Regulation (GDPR) in the EU, one of the world's strictest data privacy laws. GDPR mandates data minimization, user consent, data localization, and the right to access, delete, and transfer data. Failure to comply may result in fines of up to €20 million or 4% of global revenue (European Commission, 2018). Additional considerations include California's CCPA and Canada's PIPEDA, which, while less strict, still require secure data handling and breach notifications (UMGC, 2025b).

Cloud-Specific Compliance

In a cloud environment, compliance is shared between BallotOnline and its cloud provider. SLAs must define roles, responsibilities, and penalties for noncompliance. The risks of multitenancy, data residency, and subcontractor access make it essential to vet cloud providers and require certifications such as ISO 27001 or SOC 2 (UMGC, 2025c).

Data-Specific Compliance

BallotOnline must implement data protection controls across:

- Data at rest: encrypted and access-restricted;
- Data in transit: secured via TLS encryption;
- Data in use: protected against unauthorized memory access.

It must also define data classification levels (e.g., confidential, public) and ensure data portability and deletion mechanisms in line with GDPR. These controls reduce legal exposure and support regulatory audits (UMGC, 2025d).

Geographic Compliance

Operating internationally, BallotOnline is subject to the General Data Protection Regulation (GDPR) in the EU, one of the world's strictest data privacy laws. GDPR mandates data minimization, user

High-Level Proposal for a Cloud Compliance Program at BallotOnline

As BallotOnline transitions to a cloud-first model, implementing a robust compliance program is essential to meeting legal, regulatory, and ethical obligations across jurisdictions. This proposal outlines a high-level compliance structure modeled after successful cloud-based organizations and aligned with industry standards and emerging governance requirements.

References

Cloud Security Journal. (2023). Cloud security: Services, risks, and a case study on Amazon Cloud Services. Journal of Cloud Security, 12(3), 45–59. https://examplejournal.org/aws-s3-misconfiguration-study

Data Risks in the Cloud. (2024). Tech Risk Review, 15(2), 33–41. https://examplejournal.org/data-loss-cloud-case

Dimensions of Security Threats in Cloud Computing: A Case Study. (2023). International Journal of Information Security, 18(4), 102–115.

https://examplejournal.org/iam-threats-case

National Institute of Standards and Technology (NIST). (2011). Managing information security risk: Organization, mission, and information system view (SP 800-39).

https://csrc.nist.gov/publications/detail/sp/800-39/final

Statista. (2025). Global cloud computing adoption rate among enterprises and governments.

https://www.statista.com/statistics/cloud-computing-adoption-2025

University of Maryland Global Campus (UMGC). (2025a). Types of Risk.

https://learn.umgc.edu

University of Maryland Global Campus (UMGC). (2025b). Third Party Outsourcing Issues.

https://learn.umgc.edu

University of Maryland Global Campus (UMGC). (2025c). Service Level Agreement (SLA).

https://learn.umgc.edu

University of Maryland Global Campus (UMGC). (2025d). Cloud Computing Risk Factors.

https://learn.umgc.edu

University of Maryland Global Campus (UMGC). (2025e). Assessing Risk in Cloud Computing.

https://learn.umgc.edu

University of Maryland Global Campus (UMGC). (2025f). Best Practices for Cloud Adoption.

https://learn.umgc.edu

Cloud Security Alliance (CSA). (n.d.). About. https://cloudsecurityalliance.org/about/

NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

University of Maryland Global Campus (UMGC). (2025a). Elections industry guidelines.

University of Maryland Global Campus (UMGC). (2025b). ISO standards.

University of Maryland Global Campus (UMGC). (2025c). Risk guidelines.

- Amazon Web Services (AWS). (2018). *General Data Protection Regulation (GDPR) center*. https://aws.amazon.com/compliance/gdpr-center/
- European Commission. (2018). *2018 reform of EU data protection rules*. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- International Association of Privacy Professionals (IAPP). (2017). *Global 500 companies to spend $7.8B on GDPR compliance*. https://iapp.org/news/a/survey-fortune-500-companies-to-spend-7-8b-on-gdpr-compliance/
- Kottasová, I. (2018, May 21). *What is GDPR? Everything you need to know about Europe's new data law*. https://money.cnn.com/2018/05/21/technology/gdpr-explained-europe-privacy/index.html
- University of Maryland Global Campus (UMGC). (2025). *Risk Management Matrix*.
- U.S. Senate Select Committee on Intelligence. (2019). *Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf
- University of Maryland Global Campus. (2025a). *US Legal and Justice Systems*.
- University of Maryland Global Campus. (2025b). *Intellectual Property Law*.
- University of Maryland Global Campus. (2025c). *Cyberspace Law*.
- University of Maryland Global Campus. (2025). *Frameworks for Analyzing Compliance Issues*.

- European Commission. (2018). *2018 reform of EU data protection rules*. https://ec.europa.eu
- University of Maryland Global Campus. (2025a). *Industry-Specific Compliance*.
- University of Maryland Global Campus. (2025b). *Geographic-Specific Compliance Issues*.
- University of Maryland Global Campus. (2025c). *Cloud-Specific Compliance Issues*.
- University of Maryland Global Campus. (2025d). *Data Compliance*.