Cloud Infrastructure Design for Nonprofit Organization Project for Pride in Living (PPL)

Ngsnet Hawarya

Saint Mary's University of Minnesota

Cyber 606: Cloud Architecture

Dr. Mary Dunphy

December 21, 2024

Nonprofit organizations increasingly rely on digital systems to deliver services, manage sensitive data, and maintain operational efficiency. However, limited budgets, regulatory obligations, and staffing constraints make cloud adoption especially challenging for nonprofits. This paper presents a cloud infrastructure design proposal for Project for Pride in Living (PPL), a nonprofit organization focused on providing housing stability, employment readiness, and supportive services for individuals and families with lower incomes. The proposed architecture emphasizes security, availability, scalability, and cost efficiency while aligning with PPL's mission and operational realities. The design adopts a hybrid cloud model using secure identity management, segmented networks, encrypted storage, and compliance-focused controls. This paper explains the organizational context, requirements, architectural decisions, security controls, governance model, and implementation considerations, demonstrating how a thoughtfully designed cloud infrastructure can strengthen nonprofit service delivery while protecting sensitive data.

Introduction

Nonprofit organizations face increasing pressure to modernize their information technology environments while operating under strict financial and regulatory constraints. As service delivery becomes more data-driven and remote work becomes more common, cloud computing offers nonprofits an opportunity to improve scalability, availability, and collaboration without the overhead of maintaining extensive on-premises infrastructure. At the same time, nonprofits often handle highly sensitive information, including personally identifiable information, financial records, and health-related data, which requires strong security and governance practices.

Project for Pride in Living (PPL) is a nonprofit organization whose mission centers on building hope, assets, and self-reliance for individuals and families with lower incomes. To support this

mission, PPL relies on digital systems for case management, donor tracking, financial operations, and internal collaboration. This paper proposes a secure and cost-conscious cloud infrastructure design tailored to PPL's operational needs. The goal is not only to migrate systems to the cloud, but to design an architecture that aligns with nonprofit values, supports long-term sustainability, and protects the communities PPL serves.

Organizational Background and Technology Context

Project for Pride in Living operates across multiple program areas, including housing services, employment support, and community development. These programs require staff to access shared systems securely from different locations, including office environments and remote settings. The organization must also support collaboration between departments while maintaining strict access controls to protect sensitive client and financial data.

Like many nonprofits, PPL operates with limited IT staffing and budgetary resources. Technology decisions must therefore prioritize simplicity, reliability, and cost transparency. Cloud services provide an opportunity to reduce the burden of hardware maintenance, enable predictable operational costs, and scale resources based on actual usage. However, cloud adoption must be approached carefully to avoid misconfigurations, uncontrolled spending, and security gaps.

Cloud Infrastructure Requirements

The cloud infrastructure design for PPL is guided by several core requirements. First, the environment must ensure confidentiality, integrity, and availability of sensitive data. This includes strong identity management, encryption, and monitoring capabilities. Second, the

architecture must be cost-effective and scalable, allowing PPL to expand services without significant upfront investment. Third, the system must support compliance with applicable regulations and best practices related to data protection and nonprofit governance. Finally, the infrastructure must be manageable by a small IT team, emphasizing automation and clear governance controls.

Cloud Service Model Selection

A hybrid cloud approach is recommended for PPL to balance flexibility and control. Core applications such as email, collaboration tools, and document management are well suited for Software as a Service platform, reducing administrative overhead. Infrastructure as a Service component can be used for custom applications, databases, and legacy systems that require greater configuration control. Platform as a Service offering can support application development and integration while reducing maintenance complexity.

This layered approach allows PPL to leverage managed services where appropriate while retaining the ability to customize systems that directly support mission-critical operations. It also reduces reliance on on-premises infrastructure, lowering long-term maintenance costs.

Proposed Cloud Architecture Design

The proposed architecture is built around a secure virtual network environment segmented into distinct tiers. A virtual private cloud hosts application servers, databases, and management services. Network segmentation separates public-facing services from internal systems, reducing the risk of lateral movement in the event of a security incident.

Identity and access management is centralized using a cloud-based directory service integrated with multi-factor authentication. Role-based access controls ensure that staff can only access systems relevant to their job responsibilities. This design aligns with the principle of least privilege and supports auditing and accountability.

Data storage services are configured with encryption at rest and in transit. Automated backups and replication across availability zones improve resilience and disaster recovery capabilities. Monitoring and logging services provide visibility into system activity and support incident detection and response.

Security Controls and Risk Management

Security controls within a nonprofit cloud environment must be intentionally designed to balance strong protection with operational simplicity. For Project for Pride in Living (PPL), risk management begins with recognizing that the organization handles sensitive client information, donor financial records, and internal operational data. A defense-in-depth strategy is therefore essential. This approach layers multiple security mechanisms so that the failure of a single control does not result in a system-wide compromise. In cloud environments, risk often increases because “essential services are often outsourced to a third party,” which can complicate security, availability, and compliance responsibilities (Hashizume et al., 2013, para. 1).

At the network level, security is enforced through virtual firewalls, network security groups, and subnet segmentation. Public-facing services, such as web portals or externally accessible applications, are isolated from internal systems that store sensitive data. This segmentation limits lateral movement if an attacker gains initial access. Network traffic is monitored using intrusion

detection and prevention systems to identify suspicious patterns, unauthorized access attempts, or anomalous behavior.

Identity and access management represents one of the most critical security layers in the proposed design. Centralized identity services are integrated with multi-factor authentication to reduce the risk of credential compromise. Role-based access control ensures that staff members only have access to systems and data required for their job functions. For example, program staff may access case management systems but not financial records, while finance personnel have restricted access to accounting platforms. Regular access reviews are conducted to verify that permissions remain appropriate as roles change.

Multi-tenancy is another cloud reality that affects the risk picture. Research has shown that cross-VM side channels can create “information leakage” concerns when different customers share physical resources (Ristenpart et al., 2009). Even when such attacks are not common in day-to-day operations, they reinforce why PPL’s most sensitive workloads should use tighter segmentation, hardened configurations, and careful vendor controls.

Endpoint and device security further strengthens the overall risk posture. Devices used to access cloud systems are subject to baseline security requirements, including operating system updates, endpoint protection software, and device encryption. Secure remote access mechanisms, such as virtual private network connections or conditional access policies, are used to protect cloud access from untrusted networks. This is important because “security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall” (Ramgovind et al., 2010, p. 1).

Encryption is a foundational element of data protection within cloud architecture. All sensitive data is encrypted at rest using industry-standard encryption algorithms. Data in transit is protected using Transport Layer Security to prevent interception or tampering. Encryption keys are managed through centralized key management services, allowing for key rotation, access logging, and separation of duties. In addition, PPL should assume that threats include internal misuse at some level, since “curious or malicious administrators may capture and leak data” in hosted environments (Popa et al., 2011, p. 1). These controls collectively reduce the likelihood and impact of data breaches while supporting compliance obligations.

Compliance and Data Governance

Effective data governance is essential for nonprofit organizations that must demonstrate accountability to clients, donors, regulators, and funding partners. For PPL, compliance requirements may include data protection laws, contractual obligations with funding agencies, and internal policies governing ethical data use. The proposed cloud architecture embeds compliance into daily operations rather than treating it as a separate activity.

Governance begins with clarity on responsibilities. Cloud does not eliminate governance work; it changes where it happens. PPL still owns its data and must control who can access it, how it is used, and how long it is retained. In cloud security research, users are warned that “cloud service users need to be vigilant in understanding the risks of data breaches” in cloud environments (Subashini & Kavitha, 2011, para. 1). In practice, vigilance means formal policies, monitoring, and routine verification.

Logging and monitoring services play a central role in compliance and governance. System access, configuration changes, and data access events are logged and retained according to defined policies. These logs support audits, incident investigations, and compliance reporting. Automated alerts notify administrators of potentially unauthorized or policy-violating activity, enabling timely response.

Data classification policies guide how information is stored, accessed, and shared. Highly sensitive data, such as personally identifiable information and financial records, is subject to stricter access controls and enhanced monitoring. Less sensitive operational data can be shared more broadly to support collaboration while still maintaining appropriate safeguards. Data retention and disposal policies ensure that information is kept only as long as necessary to meet operational and legal requirements. PPL should also document how cloud features support compliance goals, since maintaining compliance can be “harder” when services are outsourced and controls are distributed across the organization and the provider (Hashizume et al., 2013, para. 1).

Governance responsibilities are clearly defined within the organization. Data owners are responsible for approving access and ensuring appropriate use, while the IT function enforces technical controls and monitors compliance. Incident response procedures outline how security events are reported, investigated, and resolved, ensuring consistency and accountability. Finally, a nonprofit context requires that compliance is not only about legal checklists. It is also about protecting clients and maintaining trust with donors and funders.

Business Continuity and Disaster Recovery

Nonprofit organizations must demonstrate responsible stewardship of donor and client data. The proposed cloud architecture supports compliance by implementing logging, access reviews, and data retention policies. Audit trails are maintained to support internal reviews and external reporting requirements.

Data classification policies guide how information is stored and accessed. Sensitive data is subject to stricter controls, while less sensitive information can be shared more broadly to support collaboration. Governance processes define responsibilities for data ownership, access approvals, and incident response.

Business Continuity and Disaster Recovery

Service availability is critical for PPL's operations, particularly for programs that support vulnerable populations. Cloud architecture includes redundancy across multiple availability zones to reduce the impact of outages. Automated backups and tested recovery procedures ensure that systems can be restored in a timely manner.

Disaster recovery planning is aligned with organizational priorities, balancing recovery time objectives with cost considerations. This approach ensures resilience without exceeding budget constraints.

Cost Management and Optimization

Cost control is a key concern for nonprofits. The proposed design incorporates budgeting tools, usage monitoring, and cost alerts to prevent unexpected expenses. Rightsizing resources and use of reserved or nonprofit-discounted pricing models further reduce costs.

By shifting from capital expenditure to operational expenses, PPL gains greater financial predictability. Regular cost reviews help ensure that cloud resources continue to align with organizational needs.

Implementation Strategy

Implementing a cloud infrastructure within a nonprofit environment requires careful planning to minimize operational disruption and manage risk. A phased implementation strategy is recommended for Project for Pride in Living to allow gradual adoption and continuous learning. The initial phase focuses on establishing foundational services, including identity management, network configuration, and baseline security controls. This phase creates a secure framework upon which additional services can be deployed.

Subsequent phases address the migration of applications and data based on risk and complexity. Low-risk systems, such as collaboration tools and non-sensitive document repositories, are migrated first to build organizational confidence and technical familiarity. More sensitive systems, including case management and financial applications, are migrated later once security controls and governance processes are fully operational.

Because cloud is often adopted for flexibility, it can be tempting to move too quickly. However, the stronger approach is to treat cloud migration as organizational change, not only a technical upgrade. Cloud research notes that cloud can reduce the need to “plan ahead for provisioning” because resources can be expanded as demand rises (Zhang et al., 2010, para. 2). For PPL, that benefit only becomes sustainable if implementation decisions are tied to governance, training, and ongoing operational procedures.

Change management is a critical component of the implementation strategy. Clear communication ensures that staff understand the purpose of the migration, expected benefits, and any changes to workflows. Training sessions and user documentation help staff adopt new tools securely and effectively. By investing in user education, PPL reduces the likelihood of security incidents caused by human error.

Ongoing operations are supported through standardized procedures for system updates, access requests, and incident response. Automation is leveraged where possible to reduce manual effort and ensure consistency. This approach allows a small IT team to manage the environment efficiently while maintaining strong security and availability.

Future Scalability and Innovation

The proposed cloud infrastructure is designed to support PPL's long-term growth and adaptability. Cloud-native services allow the organization to scale resources in response to changing program demands without significant upfront investment. As data volumes increase, storage and analytics services can be expanded seamlessly to support reporting, evaluation, and strategic planning.

Architecture also enables future innovation through secure integrations with partner organizations, government agencies, and service providers. Automation and data analytics capabilities can enhance program effectiveness and improve service delivery. By establishing a flexible and secure foundation, PPL is positioned to adopt emerging technologies while maintaining control over costs and risks.

Cloud Provider Comparison for Nonprofits Selecting an appropriate cloud service provider is a critical decision for nonprofit organizations. Two leading providers, Amazon Web Services and Microsoft Azure, offer robust platforms with nonprofit-focused programs. Both providers deliver scalable infrastructure, strong security capabilities, and global availability, but they differ in ecosystem integration and management approach.

Amazon Web Services is widely recognized for its breadth of services and maturity. AWS offers extensive infrastructure options, advanced security tools, and granular cost management features. Its nonprofit support program provides credits and discounts that can significantly reduce costs. AWS is particularly well suited for organizations requiring fine-grained control over infrastructure and custom application deployments.

Microsoft Azure offers strong integration with widely used productivity tools such as Microsoft 365. For nonprofits already relying on Microsoft platforms for email, collaboration, and identity management, Azure provides a cohesive and familiar environment. Azure Active Directory simplifies identity and access management, while nonprofit pricing programs help reduce financial barriers.

From a practical infrastructure view, major cloud platforms provide similar core capabilities: virtual machines, managed storage, identity services, logging, and security tooling. Cloud environments are attractive because they let organizations rent infrastructure dynamically; as one well-known study described cloud services “allow users to instantiate virtual machines (VMs) on demand” and purchase capacity when needed (Ristenpart et al., 2009, p. 1). For PPL, the deciding factors are therefore less about whether the provider can deliver basic cloud functions

and more about organizational fit: current skill sets, identity integration, licensing, support, and the ability to manage costs.

For PPL, the choice between AWS and Azure depends on existing technology investments and staff expertise. Azure may offer advantages in terms of user familiarity and identity integration, while AWS provides flexibility and a broad service ecosystem. Either platform can meet PPL's requirements when configured according to best practices, including strong identity controls, segmentation, encryption, and centralized monitoring.

Ethical and Social Impact Considerations

Nonprofit organizations have an ethical responsibility to protect the dignity, privacy, and trust of the communities they serve. Cloud infrastructure decisions directly affect how client data is collected, stored, and used. For PPL, ethical considerations include minimizing data exposure, ensuring transparency in data practices, and avoiding unnecessary collection of sensitive information.

The proposed cloud design supports ethical data stewardship by enforcing least-privilege access, strong encryption, and clear governance policies. These measures help ensure that technology serves the mission rather than introducing new risks. Responsible cloud adoption also supports social equity by enabling reliable service delivery and efficient use of limited resources.

Architecture Diagram Description

Although a visual diagram is not included in this paper, the proposed cloud architecture can be described conceptually. At the core is a virtual private cloud containing segmented subnets for

public-facing services, internal applications, and data storage. Identity services sit above the network layer, controlling access across all components. Security monitoring and logging services span the environment, collecting data from network, computers, and storage resources. External users access services through secure gateways, while administrators manage the environment through protected management interfaces. This layered design emphasizes clarity, security, and resilience. The proposed cloud infrastructure positions PPL to adopt new technologies as organizational needs evolve. Data analytics, automation, and secure integrations with partner systems can be introduced without major architectural changes. This flexibility supports long-term innovation and mission growth.

Conclusion A well-designed cloud infrastructure can significantly enhance the operational effectiveness of nonprofit organizations while protecting sensitive data and controlling costs. The proposed architecture for Project for Pride in Living demonstrates how cloud services can be aligned with nonprofit values and practical constraints. By emphasizing security, governance, and scalability, this design supports PPL's mission and provides a foundation for sustainable digital growth.

References

Azevedo, L. (2021). The impact of cloud management platforms on nonprofit business models. *Journal of Technology in Human Services, 39*(4), 405–425. https://doi.org/10.1080/15228835.2021.1920556

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security, 13*(2), 113–170. https://doi.org/10.1007/s10207-013-0208-7

Hackler, D., & Saxton, G. D. (2007). The strategic use of information technology by nonprofit organizations: Increasing capacity and untapped potential. *Public Administration Review, 67*(3), 474–487. https://doi.org/10.1111/j.1540-6210.2007.00730.x

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 1–13. https://doi.org/10.1186/1869-0238-4-5

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems, 51*(1), 176–189. https://doi.org/10.1016/j.dss.2010.12.006

Mayer, D. J. (2023). Exploring data use in nonprofit organizations. *Evaluation and Program Planning, 97*, 102214. https://doi.org/10.1016/j.evalprogplan.2022.102214

Popa, R. A., Redfield, C. M. S., Zeldovich, N., & Balakrishnan, H. (2011). CryptDB: Protecting confidentiality with encrypted query processing. In *Proceedings of the 23rd ACM*

Symposium on Operating Systems Principles (SOSP '11) (pp. 85–100). Association for Computing Machinery.

Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The management of security in cloud computing. In *2010 Information Security for South Africa (ISSA)* (pp. 1–7). IEEE. https://doi.org/10.1109/ISSA.2010.5588290

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: Exploring information leakage in third-party computer clouds. In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)* (pp. 199–212). Association for Computing Machinery. https://doi.org/10.1145/1653662.1653687

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006

Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: Researching desires and realities. *Journal of Information Technology, 27*(3), 179–197. https://doi.org/10.1057/jit.2012.17

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7–18. https://doi.org/10.1007/s13174-010-0007-6

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006