Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 23, 2026 | Accepted: October 28, 2026 | Publication: November 2, 2026

Cloud and DevOps operations with a governance-first approach for mission-driven institutions: a practical model for trust, auditability, and digital inclusion.

Governance-first cloud and DevOps operations for mission-driven institutions: a practical model for reliability, auditability and digital inclusion

Cloud and DevOps operations with priority in governance for mission-driven institutions: a practical model for reliability, auditability and digital inclusion

Obed Bessa Rocha da Silva

Independent Cloud Solutions Architect and DevOps Researcher

SUMMARY

Mission-driven institutions increasingly rely on cloud computing and DevOps practices; however, many operate with small teams, legacy processes, and high expectations for continuity, accountability, and public trust. This article proposes a governance-prioritized operational model for institutional cloud and DevOps environments. The model organizes practices around five mutually reinforcing capabilities: architectural baseline, operational standardization, security and auditability, observability and incident response, and workforce enablement. Instead of treating governance as a post-implementation documentation layer, the article positions it as an engineering control that can be incorporated into reference architectures, runbooks, playbooks, access routines, and continuous improvement cycles. This article is intended for IT leaders and professionals from public sector, educational, non-profit, and community-oriented organizations that need to modernize their digital infrastructure without losing traceability or operational discipline. The text synthesizes professional practice patterns in cloud architecture, DevOps, security, and reliability engineering into an applicable model adaptable to institutions with different levels of maturity.

Keywords: cloud governance; DevOps; digital infrastructure; institutional technology; reliability engineering; auditability; incident response; digital inclusion.

1 INTRODUCTION

Cloud computing and DevOps have transformed the costs and speed of digital infrastructure.

In commercial technology organizations, the prevailing narrative often emphasizes speed:

Shorter launch cycles, elastic platforms, automation, and continuous delivery. Institutions

Mission-oriented organizations face the same technical pressures, but their operational context is different.

Public bodies, educational organizations, social institutions, churches, programs without

For-profit and community initiatives often require modern infrastructure, and

At the same time, they must preserve continuity, accountability, and understandable controls.

Even without large teams specializing in platforms, their systems support services from

which people depend on.

In these environments, the central question is not simply how to migrate workloads to

Cloud platforms or automating deployments. The most difficult question is how to make them governable.

Cloud and DevOps practices: how to ensure configurations are reproducible, the

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 23, 2026 | Accepted: October 28, 2026 | Publication: November 2, 2026

incidents can be diagnosed, access decisions can be auditable, and knowledge
Operational governance should not remain restricted to the memory of a single technical leader. Governance, in
this sense, is not bureaucracy. It is the set of engineering and management practices that allows the institution to trust.
in its digital infrastructure.
This article presents a governance-first model for institutional cloud operations.
and DevOps. The model was designed for organizations that need a practical bridge between
It is not intended to replace high-level governance requirements and daily engineering work.
Consolidated standards and supplier architectures. Instead, it translates these benchmarks into
An operational model focused on reliability, security, auditability, and digital inclusion.

2. Why Governance Should Integrate Engineering Practice

Traditional IT governance often manifests itself in policy documents, points
Formal approval processes and periodic reviews. These instruments remain useful, but they are...
insufficient in cloud and DevOps environments, where infrastructure can be changed.
Quickly, access can be delegated between services, and configuration deviations can occur without...
visibility. A governance system restricted to documents tends to become outdated compared to a system that...
should control.
An operational model that prioritizes governance incorporates governance into the workflow.
engineering. It requires teams to define reference architectures before deployments.
hoc, codify reproducible configuration patterns, document incident routines before the
emergencies and integrate records, permissions, backup routines, and change histories at the surface.
normal design practice. This guideline follows the broader movement toward safety.
From conception to reliability engineering and continuous compliance.
This need is especially evident in institutions with social or public missions.
A small organization may not describe its work as platform engineering, but
It still needs reliable identity management, backup discipline, access review, and inventory.
of assets, continuity of services, and technical training. When these practices are absent, the
Modernization can increase risk: the institution acquires new tools, but loses clarity.
operational.

3. The Governance-Prioritized Model

The proposed model brings together five capabilities. Each one can be implemented incrementally.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 23, 2026 | Accepted: October 28, 2026 | Publication: November 2, 2026

But the most robust results emerge when they reinforce each other. The baseline of Architecture defines the desired operational model. Operational standardization transforms this. A model based on reproducible routines. Security and auditability make decisions traceable. Observability and incident response ensure that failures can be detected and managed. Workforce training makes the model sustainable by converting technical knowledge into shared institutional capacity.

Table 1 – Capabilities of the governance-prioritized model for institutional operations cloud and DevOps

Capacity	Practical Controls	Institutional Result
Architectural baseline	Reference architectures, environment classification, backup and recovery objectives, identity model, and service responsibility.	A shared map of the institution's digital infrastructure and risk posture.
Operational standardization	Operational guidelines, response plans, configuration standards, change management routines, asset inventory, and supplier management and service level agreements (SLAs).	Less variability, faster integration, and less reliance on undocumented knowledge.
Security and auditability	Least privilege access, periodic access review, logging requirements, evidence retention, and mapping between policies and controls.	Traceable decisions and greater preparedness for internal reviews or external.
Observability and incident response	Monitoring, forwarding of alerts, review of records, incident severity levels, post-incident review, and service integrity indicators.	Faster diagnosis, more disciplined recovery, and learning from mistakes.
Workforce training	Applied training, documentation habits, digital inclusion initiatives, and role-based technical guidance.	Sustainable operations and broader participation in digital transformation.

3.1 Architecture Baseline

An architectural baseline constitutes the minimum feasible and reliable representation of the environment. The institution's technological infrastructure. It identifies critical services, responsibilities, dependencies, environments, Access models, recovery expectations, and known risks. In cloud environments, the line The basic framework should also cover the account or project structure, network segmentation, and boundaries. identity, default registration settings, backup responsibilities, and conditions in

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: October 23, 2026 | Accepted: October 28, 2026 | Publication: November 2, 2026

Managed services are preferable to components managed by the institution itself.
The baseline should be simple enough to be maintained. A common mistake is producing a
The architectural document is too extensive to be updated. For smaller institutions, a
A compact reference architecture, a service catalog, and a decision log can offer
It offers more practical value than a comprehensive but outdated architecture repository.

3.2 Operational Standardization

Operational standardization translates architecture into reproducible practices. Operational guidelines.
Runbooks and playbooks are central artifacts. An operational guide describes
how to perform a known task, how to integrate a user, restore a backup, renew a
to credential or validate a deployment. A response plan describes how to react to a class of
events, such as service unavailability, suspected account compromise, or problems with
data integrity.
Standardization does not eliminate professional judgment. It reduces the number of situations in which...
Decisions need to be made under pressure and with incomplete information. It also creates a basis.
Training for less experienced team members, promoting digital inclusion within
from the institution itself.

3.3 Security and Auditability

Security and auditability should be treated as engineering requirements. Access controls,
Event logging, evidence retention, and configuration review need to be defined beforehand.
that a system becomes critical. The NIST Cybersecurity Framework 2.0 highlights governance as
A central function that determines how cybersecurity risk is understood and managed.
In institutional settings, this means that technical teams must be able to explain no.
It's not just a question of whether a particular control exists, but why it exists, who is responsible for it, and how it works.
Evidence of its operation is preserved.
The principles of zero trust are useful because they promote explicit verification and least privilege.
and continuous evaluation of trust relationships. For smaller organizations, the practical starting point
It can be modest: centralize identity, eliminate shared accounts, document access.
privileged and review permissions periodically.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 23, 2026 | Accepted: October 28, 2026 | Publication: November 2, 2026

3.4 Observability and Incident Response

Observability provides the necessary signals for managing reliability. Monitoring and
Event logging should be aligned with the criticality of the service. Not every system requires it.
same level of instrumentation, but each critical service must have a person responsible, a definition of
Integrity, alert expectations, and an incident handling workflow. Engineering of
Website reliability has popularized service level objectives and error budgets as...
ways to connect engineering work to the reliability perceived by the user. Even when
Even if an institution does not formally adopt SRE (Systematic Reliability Evaluation), the principle remains valid: reliability must be...
described in terms relevant to the people who depend on the service.
Post-incident review is equally important. A review prioritizing governance is not...
It is limited to the technical cause. It assesses whether the organization had adequate detection procedures,
documentation, access, backup, scaling, and communication. The result should be a set
reduced improvements whose progress can be tracked until completion.

3.5 Workforce Training and Digital Inclusion

Digital inclusion is often discussed as access to technology by external communities.
Institutions also need internal digital inclusion: employees and volunteers should
to understand the systems they use, the risks they manage, and the routines that maintain the services.
Reliable. Training must therefore be linked to operational tools. A guide
Operational control is not just a tool; it's also a learning tool. A response plan.
It's not just a tool for incidents; it's also a way to distribute capacity.
judgment by the entire organization.
This perspective is particularly important in mission-driven organizations, in which the
Technological work often transcends the formal boundaries of job titles. The goal is not...
To transform each stakeholder into an engineer. The goal is to create shared understanding.
sufficient for technological decisions to become more transparent, resilient, and aligned with
institutional purpose.

4. IMPLEMENTATION ROADMAP

Organizations can adopt the model through a step-by-step roadmap. The roadmap is...
intentionally light, as many institutions cannot interrupt their operations to perform

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: October 23, 2026 | Accepted: October 28, 2026 | Publication: November 2, 2026

a broad transformation program.

• Step 1: Establish the baseline. Identify critical services, responsible parties, dependencies, and accounts. privileged resources, backup routines, and unresolved risks.

• Step 2: Standardize the most frequent tasks. Create concise operational guides for integration of Users, access changes, backups, recovery checks, and routine maintenance.

• Step 3: Define incident classes. Agree on severity levels, escalation flows, Communications, evidence gathering, and expectations for post-incident reviews.

• Step 4: Incorporate security and auditability. Map policies to controls, schedule reviews of Access, preserve critical system records, and document exceptions.

• Step 5: Teach the operational model. Use operational guides, response plans, and lessons learned. incidents as training materials for technical and non-technical stakeholders.

The roadmap should be evaluated based on its operational maturity, not the volume of documentation. Useful indicators include the team's ability to identify those responsible for the services, restore a critical backup, explain privileged access, reproduce a configuration, forward an incident and empower a new participant without relying entirely on informal memory.

5 RISKS AND REWARDS

The governance-prioritized model involves trade-offs. Excessive standardization can... Delaying experimentation. Insufficient standardization can make systems fragile. Balance Appropriateness depends on institutional risk, the criticality of services, and the maturity of the team. A useful rule is to standardize the points where a failure would cause institutional damage and preserve the Flexibility where learning is the main objective.

Another risk is purely performative governance: producing documents that meet a checklist. audit verification, but do not influence operations. This risk can be reduced. linking each governance artifact to an operational routine. A policy should correspond to a control; a control must correspond to evidence; and the evidence must be able to be recovered by the people responsible for the service.

6 CONCLUSION

Cloud and DevOps practices can help mission-driven organizations modernize their Infrastructure, but modernization without governance can increase fragility. A model Operational governance, with a focus on reliability, security, auditability, and...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: October 23, 2026 | Accepted: October 28, 2026 | Publication: November 2, 2026

Knowledge transfer as an engineering responsibility. By incorporating governance into
reference architectures, operational guides, response plans, access routines, observability
With training and capacity building, institutions can create a digital infrastructure that is not only modern, but also
Understandable and reliable.

The model presented is intentionally practical. Its value does not lie in adding yet another [feature/function].
not just a layer of terminology, but in helping institutions develop reproducible habits that
Protect continuity and expand participation in digital transformation.

ACKNOWLEDGEMENTS

The author used OpenAI ChatGPT as support in writing, structural refinement, and...
Editorial organization. The author has reviewed and revised the manuscript and assumes responsibility for its
Final content. The article does not include figures, images, or experimental data generated by artificial intelligence.
artificial.

REFERENCES

[1] IEEE Computer Society, “Author Information: IT Professional.” [Online]. Available at: https://www.computer.org/csdl/magazine/it/write-for-us

[2] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST, Feb. 2024. [Online]. Available at: https://www.nist.gov/cyberframework

[3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, Aug. 2020. [Online]. Available at: https://doi.org/10.6028/NIST.SP.800-207

[4] B. Beyer, C. Jones, J. Petoff and NR Murphy, Site Reliability Engineering: How Google Runs Production Systems. Sebastopol, CA, USA: O'Reilly Media, 2016. [Online]. Available at: https://sre.google/sre-book/table-of-contents/

[5] AWS, “AWS Well-Architected Framework.” [Online]. https://docs.aws.amazon.com/ Available at: wellarchitected/latest/framework/welcome.html

[6] Google Cloud, “DORA: DevOps Research and Assessment.” [Online]. Available at: https://dora.dev/

[7] Cloud Security Alliance, “Cloud Controls Matrix.” [Online]. Available at: https://cloudsecurityalliance.org/research/cloud-controls-matrix

[8] IEEE, “IEEE Submission and Peer Review Policies.” [Online]. Available at: https://journals.ieeeauthorcenter.ieee.org/submit-your-article-for-peer-review/ieee-submission-and-peer-review-policies/

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.