Industry White Paper

Future Proofing Your IT Infrastructure:
New Infrastructure Requires New Governance

Closed Loop Lifecycle Planning©
In collaboration with HP®, Microsoft®, and Intel®

April 2025

Submitted by: Jeff Malec, HP Principal Technologist and Lifecycle Subject Matter Expert
Bruce Michelson, Distinguished Technologist Emeritus HP
Close Loop LLC, Manager

Table of Contents

About the Authors

Jeff Malec

Jeff Malec is an HP Principal Technologist and Lifecycle Planning Subject Matter Expert. After a 21+ year career with Microsoft, Jeff joined HP and is driving adoption of the modern workplace, Windows 11, and the related lifecycle elements.

Managing the Microsoft and HP relationship for several years, Jeff is an expert in go to market plans and customer adoption strategies.

Jeff holds multiple technical certifications from Microsoft.

Bruce Michelson

Bruce Michelson is an HP Distinguished Technologist (Emeritus) and the Manager of Close Loop LLC. Bruce has over 36+ years in delivering industry white paper and customer engagements. Bruce has delivered over 1,000+ white papers and over 350+ engagements.

Bruce is the author of seven books regarding aspects of lifecycle management. Bruce has numerous copyrights and patents regarding his expertise in User Segmentation, lifecycle management, cost of change, The Ready State©, and Appropriate Incumbent Behavior©.

Bruce teaches IT in Health Care and Advanced Systems and Design at Florida Atlantic University where he is an adjunct.

Bruce is sponsored by the HP, Microsoft, and Intel Alliance for this engagement.

1.0 Management Summary

As a concept, Future Proofing is about assuring that the next generation of the IT infrastructure is appropriately planned, designed, implemented and maintained (the PDIM methodology).

Closed Loop Lifecycle Planning© defines Future Proofing as "the methodology that an organization leverages to embrace, accommodate, and manage technology innovations in the IT infrastructure."

Many organizations view Future Proofing not as a discipline or methodology, but merely a part of continuous process improvement. That perspective minimizes the potential impact and implications of Future Proofing. Future Proofing represents a significant change in the IT infrastructure—a "sea change."

The pace and scope of the innovations whether it is modern management, AI, the cloud, or advance automation in general represents one of the most significant governance challenges ever faced. The technologies that are being implemented simply did not exist in the manner, scope, and complexity that they exist in this post-pandemic era.

With the changing demographics in the workforce and the focus on the digital end user experience, the end users will drive relentless change to the IT infrastructure. We are now dealing with the most technical savvy workforce ever with end users who have been leveraging technology of all kinds from a very early age. Technology is now an expectation and a requirement.

The focus is not the traditional recruit, attract, and retain top talent, it is really about remaining competitive in an era where technology is a differentiator.

Governance is one of the keys, if not the primary key, to successfully and securely embrace all of the technology changes that are occurring.

Governance must be created, embraced and adopted *before* all of this new innovation is implemented. Implementing governance post-implementation represents risk and Tech Debt.

1.1 Objectives of this White Paper

This White Paper focuses exclusively on governance as it related to the changing IT infrastructure. Each section of this White Paper focuses on a particular aspect of the overall governance.

As Closed Loop Lifecycle Planning has concluded "no one likes governance."

Governance is often avoided or deferred as much as possible. Perhaps the avoidance is due to all of the constituencies that must be involved or perhaps trying to build a consensus on guardrails. Whatever the rationale, the trend seems to be undeniable, although many will disagree.

Another challenge with governance has always been the consequences of not adhering to the governance model. Governance should equally apply to all end users regardless of their personas or role in the organization. Consequences must align to the impact of not following the governance model.

This is a polite way of stating that a “slap on the wrist” for non-adherence to governance is “worthless” and not meaningful. Consequences should be defined and communicated at the same time the governance is created, not after the fact.

A key objective of this White Paper is to provide guidance that all of the lifecycle pillars are and should have a governance model in place.

1.2 Governance as Tech Debt

The technology that is being deployed today, both the elements themselves and how they are delivered and deployed, did not exist in the same manner as they do today. The new IT infrastructure requires a new set of governance, not a re-do of the previous governance models. Security, cost, and end user experience demands this approach.

Given the pace of technology changes, governance should be constantly aligned to the new technology’s contempt.

Trying to manage this new technology whether it is AI, NPU, “as a service,” cloud, etc. with an outdated playbook (i.e., governance) is inviting negative impact and implications.

Governance is Tech Debt if the current and future states are not fully aligned to the strategies and technologies in the IT infrastructure.

1.3 The Governance Gap

It is reasonable to sate that every organization has an element of governance as Tech Debt. A few brief Closed Loop Lifecycle Planning observations will assist in validating this point of view.

A basic example is pilots and proof of concepts (PoCs). As PoCs are delivered, it is common that governance is not a part of the success criteria. In other words, the technology is assessed but not the guardrails on how that technology is to be leveraged. Governance incudes the policy, process, and procedures that provide the security and foundation for that technology use case.

Many organizations do not view governance as a part of the on-going process. Annual audits or systems reviews do not necessarily examine governance in detail with specificity in terms of assessing if the governance in place addresses all of the elements of the new IT infrastructure.

Governance has always been challenged and usually lags behind technologies, according to the closed Loop Lifecycle Planning conclusions. In this era of rapid acceleration of innovation, security would seem to demand the attention recognizing that governance equals security.

The governance gap has been around quite a while, often with only a breach or negative event to drive change. The governance gap remains a significant gap for most organizations.

1.4 Business vs. Technical Governance

One factor contributing to the governance gap is the process by which governance is established. The team responsible for creating governance often focuses on business aspects, generally at a higher level. Given the complexity of modern technology and its integration into workflows, a technical background is crucial alongside a business background.

A person without comprehensive understanding of new technologies may not be fully qualified to develop a governance model without input from a teammate who can address the technical requirements. Effective governance requires multiple skill sets to establish appropriate guardrails for the technologies under consideration.

2.0 Governance - Hardware

Hardware is like the starting point for governance for most organizations. Establishing hardware standards has been a part of It for decades. Today, the configuration management is significantly different that its previous definition just a few years ago.

Simply stated, new hardware alternatives require new governance.

Configuration management now includes:

- AI whether it is driven by hardware (NPUs) or CPU/GPU
- AI whether it is embedded in the operating system
- AI elements included in the OEM client design and features
- Components and peripherals such as audio and video

The point is that the product portfolio includes new elements that require governance for compliance, security and management. Previous governance did not include, nor anticipate, such inclusion and integration into the client hardware standards.

3.0 Governance - Software

Many organizations have not identified elements of the software portfolio as lacking in governance. However, if the software processes are the same as pre-pandemic, as the timeline, then there is a governance gap.

There are elements that require new governance to address issues that simply did not exist before. Below is a brief listing of 4 elements provided a representative example of those points:

- Software In-Take

Software In-Take is the process that new software titles and versions are added incrementally to the organization installed base. For many organizations today, Software In-Take is the same as it has been previous. With new modules that could have AI built in or other technologies embedded, the In-Take process should be reviewed for current threats as well as how the software now works.

- Software Ownership

  Software Ownership has rarely changed to keep up with the times. Software Ownership requires a new, modern definition with roles and responsibilities clearly defined and meaningful. Software Ownership often comes with privileges for downloads and adoption which requires signing terms and conditions, which generally are restricted in an organization.

- ISV Modules

  New modules of existing software and net new modules require new rigor before adoption. This is a solid example where the Software Ownership (typically a business owner, not a technical owner) may not be skilled to fully "own" the solution under consideration.

- Version Control

  Version control (or lack thereof) is a by-product of the lack of governance. Aside from represent security issues, performance issues, among other implications, version control represents a new need for an N-X strategy. The question has always been, "how many versions of a software suite is required and what are the implications?"

- APIs

  APIs have become an area of target for the bad actors. Often associated with legacy, APIs represent an attack vector that is being exploited. New governance is required to assure that APIs are modern, up to date, and secure.

- Updates

  As we learned from Blue Screen Friday, updating software requires increased due diligence. An outage driven by the timing and scope of an update can represent the equivalent downtime to a disaster or breach. Having current detailed governance in place is one of the lessons learned.

4.0 Governance - Services

A change in the services portfolio including changes in the service delivery strategies requires new governance specific to the new services.

Services represents change, sometimes perceived as a “small” change and sometimes it is “large.” “Small” change could include new services, entitlements, or out tasking services to a service provider. Scope determines whether a change is “small” or “large” - however, both require new governance.

“Large” changes would include scaled out tasking, outsourcing, contracting, or hybrid services. In sourcing changes can also be significant.

The point to be made in regard to service is that services levels must be defines (SLAs/OLAs) and governance created to effectively manage that service. The SLA/OLA is simply not enough, there must be governance associated with changes in the service strategies.

5.0 Governance - Cloud (Modern Management)

Closed Loop Lifecycle Planning defines modern management as “the cloud first, highly automated, highly secure IT infrastructure built around the end user requirements.”

As an organization migrates from an on-premises to a cloud-based solution, or a combination of both alternatives (hybrid) the governance is clearly different and roles and responsibilities are changed. The governance needs to reflect the change in service delivery strategies.

The roles and responsibilities must be defined and if cloud based to a provider, the new governance should reflect both the internal and external governance. The governance for cloud should be documented and approved before that migration with consequences if the governance is not followed and adhered. Periodic and timely audits will need to be a part of that rigor, just as any outsourced relationship.

6.0 Governance - Management Tools

Every organization possesses a portfolio of security and manageability tools. As infrastructure evolves, these suites of security and management toolsets should adjust to align with governance.

Existing management tools should not be presumed sufficient for new changes to the IT infrastructure. Governance should be established to continuously assess toolsets to align with the changes in elements discussed in this White Paper, and beyond.

The next generation of security and management tools may have a foundation in AI for security purposes as well as manageability. Self-remediation is likely to be part of that solution. Governance must remain involved in the overall process.

7.0 Governance - Disaster Recovery

There must be a new definition of a disaster. Legacy thinking often associates disaster recovery with natural disasters. While addressing these remains essential, it is imperative to also define and govern the new generation of disasters similarly.

Cyberattacks such as ransomware attacks, denial of service attacks, wiper attacks, and other forms of cyber threats can have the same impact on an organization as natural disasters, particularly in terms of organizational recovery.

Governance should encompass all types of disasters, whether natural or human caused. The roles of the recovery team, crisis recognition, and other relevant conditions should be aligned under unified governance to prevent internal competition for responsibilities during a disaster.

Response times and remediation periods should be integral components of disaster plans, and simulations reflecting new threats should be conducted regularly.

8.0 Observations and Conclusions

Governance must be further developed and enhanced as IT infrastructure evolves and expands beyond traditional models. The term "transformation" is often used to describe cloud-based models, and "digital transformation" is even more frequently mentioned. Without a corresponding governance model, these terms are meaningless.

As IT infrastructure changes, the associated guidelines must also adapt. Both elements must coexist unless an organization is prepared to face potential negative consequences. Some organizations are adopting new technologies, service delivery strategies, and approaches that significantly alter the IT infrastructure without documenting how these changes will be governed.

In the post-pandemic era, governance must be redefined to become a fundamental part of every discussion. Governance affects various aspects of the end-user environment, including security, disaster recovery, user experience, system performance, software, and software ownership. It is essential for governance to be a core competency of every organization to enable innovation with reduced risk and faster implementation times.

The primary method to achieve this goal is to elevate governance to its former position as a central element of organizational culture.

Appendix

1. Closed Loop Lifecycle Planning - A Complete Guide to Managing Your PC Fleet, Bruce Michelson, published by Addison-Wesley Division of Pearson Education, ISBN 978-0-321-47714-9.
2. Appropriate Incumbent Behavior©, copyright Bruce Michelson.

Other Books by Bruce Michelson

1. Closed Loop Lifecycle Planning©, Client Computing in the Health Care Industry, by Bruce Michelson, Published by IDG, ISBN 978-1-61623-045-6.

2. Closed Loop Lifecycle Planning© - What It Is and Why It Is Important to You, by Bruce Michelson, Published by Bookmasters, ISBN 0-9667607-0-0.

3. We Are All Retail, The Race to Improve the Retail Experience in a Post Covid World, by Bruce Michelson and Leif Olson, Published by Archway Publishing, ISBN 978-1-6657-3394-6.

4. IT Strategies in the Post-Pandemic Era, Part of the Closed Loop Lifecycle Planning© Series, published by Archway Publishing, March 2023, ISBN 978-1-6647-3856-9.

5. Zero Trust, by Bruce Michelson and Cody Gerhardt, published by Archway Publishing, May 2023, ISBN 978-1-6657-4191-0.