IOT Microsoft Low Code/No Code Center of Excellence

Governance Committee Framework

August 2023

Table of Contents

The IOT LCNC Center of Excellence Governance Committee

The CoE Governance Committee is a cross-functional team consisting of seven members, each representing diverse areas of expertise. This team is tasked with the responsibility of coordinating and customizing CoE policies and governance practices to directly meet the specific needs, requirements, and overarching goals of IOT. By effectively aligning the CoE's operational guidelines with IOT's strategic objectives, this collaborative team plays a pivotal role in ensuring seamless integration and successful implementation of CoE initiatives.

Governance Committee Members	
IOT CoE Co-Chairperson - Robert Evans	**IOT CoE Co-Chairperson** - Ann Walker
INDOT Representative - Melanee Habig	**IOT Power Platform Product Owner** - Lawrence Gibson
FSSA Representative - Derrick Cash	**IDOH Representative** - Angelo Soto

The CoE Sponsor is also the Governance Committee Sponsor, Larry Jenkins. The Sponsor will provide oversight and be involved in escalations as needed.

Governance Committee Roles

CoE Governance Committee Chair: CoE owner and responsible for bringing forward any issues to the committee and communicating governance decisions

Agency Representatives: Provide perspective of the state agencies to promote Microsoft LCNC growth and ongoing refinement of the CoE governance guidelines

IOT Representatives: Liasion with the product owner, IOT CoE's, and technology teams.

Governance Committee Responsibilities

The Governance Committee plays a crucial role in ensuring collaboration between state agencies and the LCNC CoE. Their primary duty involves establishing and overseeing LCNC governance practices to align with regulations and enhance compliance. They advise on effectively addressing non-compliance issues and confirm adherence through regular checks. Additionally, the Committee drives the adoption of the IOT CoE LCNC Delivery Framework and enterprise standards. They also provide recommendations on centralizing or decentralizing Power Platform responsibilities. Further details about responsibilities can be found in the RASCI Matrix (Appendix 1).

Governance Committee Meetings

The Governance Committee will meet on a monthly basis, adhering to the following agenda:

1. Evaluate the CoE portfolio,
2. Assess monitoring reports/KPIs,
3. Examine significant initiatives (such as refining default environments),
4. Review educational efforts.

Governance Enforcement

Policies encompass best practices and recommendations, while Standards entail business procedures or technical rules.

Governance Policies and Standards Compliance Matrix			
Impact	**Description**	**Response**	**Escalation**
Low	Policy non-compliance issue without security risk	• Address directly with agency POC	CoE Core Team
Medium	Policy or standards non-compliance issue without exposure of sensitive data	• CoE Chairpersons reports the issue to the Governance Committee (GC) • Chair communicates to agency representatives	Governance Committee
High	Standards non-compliance issue involving sensitive data and cybersecurity risk	• Chair reports the issue to the CoE Sponsor	CoE Sponsor

Technology Partners and Stakeholders

Collaboration and solution co-creation are two of the CoE's guiding principles. The CoE will have broad reach across state agencies to support, nurture and expand Microsoft LCNC solution development. Agency business and technology stakeholders have been identified to be trusted advisors and champions. Their contributions may include the following activities.

- Provides domain or technical experience to the CoE.
- Participates directly in CoE initiatives depending on the scope of the use case.
- Consult on LCNC projects depending on the scale, complexity, or risk involved in implementing the solution.
- May be involved in governance checkpoints. (i.e., license review and confirmation)
- Promote stakeholder engagement strategy using existing communications and collaboration channels. (i.e., the community of practice)
- Acts as a champion to promote the LCNC portal, celebrates successes, continues to build the community.
- Generates excitement in the newly endorsed ways of working.
- Updates the organization on what is new and what is upcoming.
- Ensures the citizen development communication channels continue to evolve in deepening community engagement and involvement.

Technology Partners and Stakeholders	
IOT CXO	License Management (Ben Hogsed)
IOT Data Exchange Team	BRM Team (Scott Sullivan)
IOT Messaging and Collaboration Team	Agencies with no IT Teams
IOT Architecture Team	Agencies with IT Teams
IOT Project Management Team	LCNC Champions Community
IOT Power Platform Technical Team (Managed through MSP)	LCNC Community of Practice

Service Management Practices

Governance and management within an organizational framework are intricately interconnected, jointly contributing to the delivery of value. While governance establishes overarching policies and standards to guide operations, management defines the specific processes and practices of which must be adhered to achieve the desired business objectives.

In this dynamic, management assumes a granular role, delving into the finer intricacies of executing within established practices. To this end, the CoE has identified eleven pivotal management practices from the ITIL 4 Service Management Model. These selected practices serve as the initial focal points for CoE governance priorities. As the CoE matures over time, the spectrum of governance priorities will inevitably broaden to mature the existing practices and encompass additional practices. As highlighted in green, Table 1 below designates the CoE's eleven chosen service management practices.

ITIL 4 Service Management Practices		
General Management	**Service Management**	**Technical Management**
Architecture Management	Availability Management	Software Development & Management
Continual Improvement	Business Analysis	Deployment Management
Information Security Management	Capacity & Performance Management	Infrastructure & Platform Management
Knowledge Management	Change Control	
Measurement & Reporting	Incident Management	
Organizational Change Management	IT Asset Management	
Portfolio Management	Problem Management	
Demand Management	Release Management	
Project Management	Service Catalog Management	
Relationship Management	Service Configuration Management	
Risk Management	Service Continuity Management	
Service Financial Management	Service Design	
Strategy Management	Service Level Management	
Workforce & Talent Management	Service Request Management	
	Service Validation & Testing	

Table 1 - The CoE'S Identified Service Management Practices

For each ITIL management practice, key governance, elements, and related metrics have been identified to facilitate the concurrent growth and alignment of the LCNC governance and delivery practices. The choice of metrics will be determined by the availability of pertinent data. The initial phase, as well as the anticipated growth of the CoE's governance, delivery Framework practices, and analytical capabilities, will be baselined in the LCNC roadmap.

For comprehensive insight, Appendix 2 provides a definition of each of the eleven practices and governance elements. These delineations offer a potential starting point and lay the groundwork for the subsequent expansion of each practice's specifics as the CoE evolves toward its targeted level of maturation.

Governance and management are inseparable partners in the pursuit of organizational value. Governance establishes the overarching direction, while management navigates the operational complexity. The CoE's strategic identification of initial management practices underscores the significance of focused governance priorities, and the eventual expansion of these practices further underscores the progressive evolution of the CoE.

IOT LCNC CoE Governance Framework

The CoE's Governance Framework encompasses a comprehensive structure that addresses leadership, organizational setups, procedures, standards, and adherence to these standards. This ensures that the CoE effectively bolsters and facilitates the realization of LCNC strategies and goals.
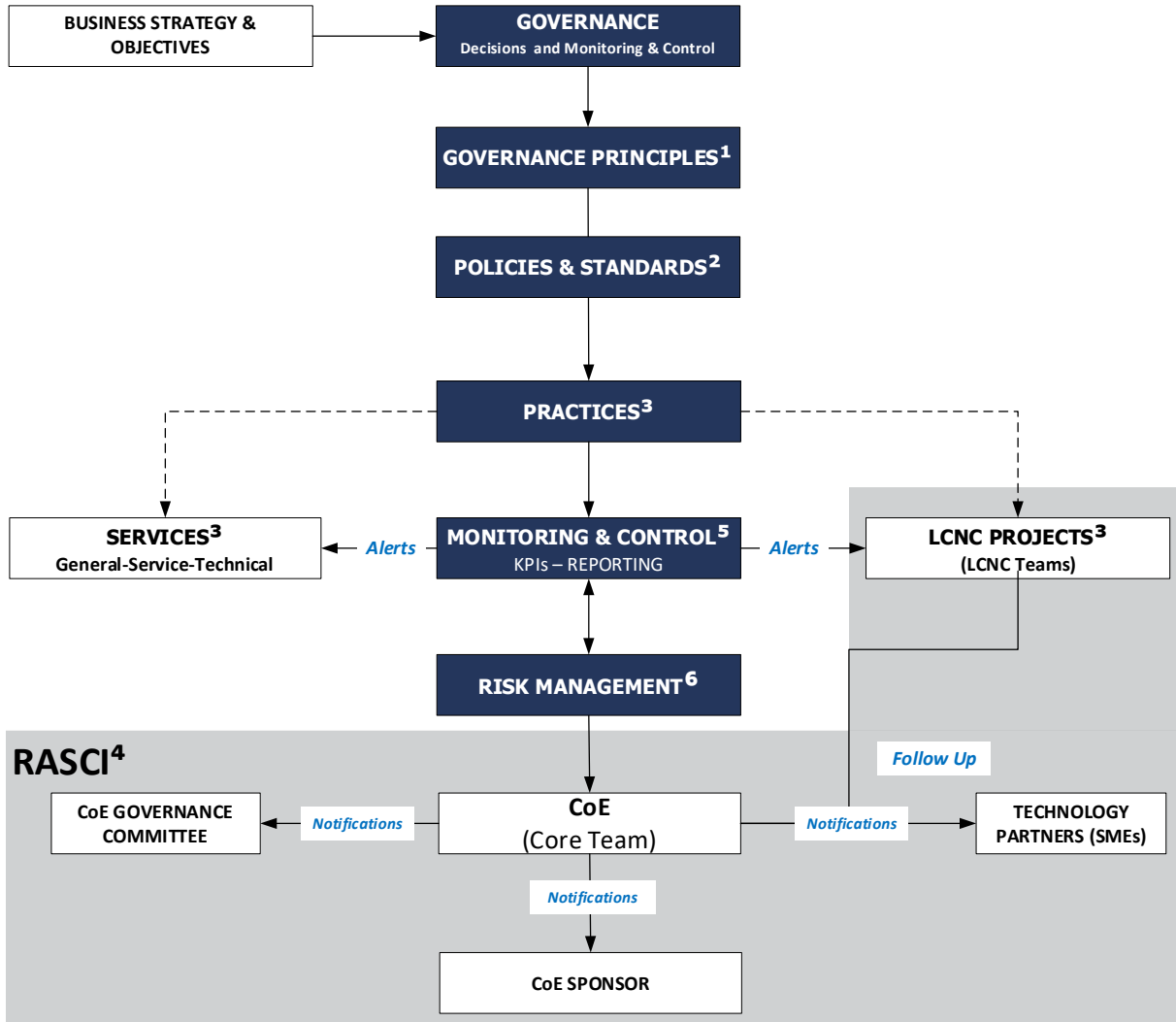

Figure 1 - CoE Governance Framework

As demonstrated in Figure 1 above, the Governance Framework includes six main components:

1. **Principles** to maintain comprehensive oversight that guide all LCNC services and projects, providing a foundation basis for their management.

2. **Policies and Standards** to establish CoE services, LCNC guidelines for management practices, and KPIs, ensuring consistency and alignment. Standardization reduces dependency on individual efforts, improves development quality, and promotes long-term maintainability.
3. **Practices** built to establish governance of development, management, and support of CoE services, LCNC projects, and the Power Platform.
4. **RASCI Matrix** helps define and communicate the roles of different individuals or groups in the execution of various governance processes or tasks.
5. **Monitor and Control** to track CoE performance and ensuring compliance with LCNC application and platform standards.
6. **Risk Management** to mitigate potential threats to the business, such as cyber-attacks, data breaches, outages, and system vulnerabilities.

1. Governance Principles

The CoE Governance Principles are fundamental guidelines that steer the decision-making and operational processes within the CoE. These principles serve as a compass, shaping how the CoE's services, projects, and activities are conducted. They provide a shared understanding of the CoE's objectives, values, and desired outcomes, which fosters consistency, transparency, and effective collaboration among stakeholders. By adhering to these principles, the CoE ensures that its initiatives align with overarching strategies and contribute to achieving organizational goals while maintaining a structured and accountable approach to its functions. The CoE's Governance Principles include the following:

- **Education:** Provide comprehensive training and educational resources aimed at enhancing the skills of LCNC developers, ensuring they are up-to-date with the latest advancements in the field.

- **Collaboration and Knowledge Sharing:** Foster collaboration and knowledge exchange among LCNC developers through platforms like forums, communities of practice, and regular meetings.

  - The CoE is responsible for clearly defining policies and standards for IT and LCNC, governing the construction, deployment, and support of secure and scalable LCNC applications.

  - The CoE will offer transparency and educational resources regarding governance policies and standards, promoting understanding and adherence.

  - The CoE, agencies, and development teams must collaborate to determine the application of rules and methods to ensure compliance.

  - The CoE will clarify the process for managing exceptions or deviations from established norms, particularly in areas such as architecture and infrastructure.

- **Standardization:** Define and promote uniform development practices, guidelines, and templates to maintain consistency and sustainability of LCNC solutions.

    o The CoE will incorporate IT policies and standards into its processes and the Power Platform architecture and administration when feasible.

    o The CoE will operationalize LCNC governance by integrating it into agency governance practices whenever feasible.

- **Security and Compliance:** Enforce adherence to security, privacy, and compliance requirements for all LCNC solutions. Regularly evaluate and mitigate associated risks.

    o IOT/CoE oversees security—not the citizen developers. This includes cyber- and data security, access and permissions, Data Loss Prevention (DLP) Policies, processes, and systems integrity policies and standards.

    o The CoE is responsible for establishing a secure and monitored environment for citizen development.

- **Continuous Improvement: Continuously** assess and enhance LCNC development processes, methodologies, and tools to optimize efficiency and efficacy.

    o Governance processes must undergo regular, impartial reviews to drive ongoing improvements.

- **MS License Consultation:** The CoE can provide guidance on Microsoft licensing requirements**.**

2. Policies and Standards

To facilitate the implementation of CoE services, practices, and Key Performance Indicators (KPIs), the CoE defines policies and standards to ensure value delivery across LCNC operations and initiatives.

Governance policies establish the operational guardrails of CoE services, detailing roles, responsibilities, and decision-making protocols. These policies create framework embracing best practices, coding standards, security measures, and design principles. By upholding these standards, the framework ensures consistent and goal-focused development of LCNC projects. Simultaneously, the framework incorporates a set of KPIs that quantitatively measure the success of LCNC initiatives. Ultimately, the CoE Governance Framework reflects the organization's unwavering commitment to excellence, unity, and strategic alignment in its LCNC journey.

Appendix 2 provides specific CoE policies and standards for each identified service management practice.

3. Practices

The Governance Framework policies and standards direct the CoE management practices. Operationalizing the management practices through the Delivery Framework ensures the governance elements are defined and measurable. These practices processes provide a clear roadmap for how the CoE operates and interacts with various stakeholders, ensuring smooth implementation of LCNC initiatives. The Framework encompasses activities such as identifying infrastructure project opportunities, prioritizing CoE led initiatives based on resourcing and strategic alignment and monitoring their progress. Additionally, the practices define how the CoE engages with project teams, communicates guidelines, facilitates knowledge sharing, and gathers feedback for continuous improvement. By adhering to these defined practices, the CoE can systematically drive the successful LCNC adoption while maintaining consistency, collaboration, and strategic alignment throughout its operations.

4. RASCI Matrix

The RASCI Matrix employed by the CoE plays a pivotal role in conveying the responsibilities encompassing diverse individuals and groups. This Matrix, structured around the "Responsible," "Accountable," "Supportive," "Consulted," and "Informed" roles, serves as a comprehensive guide to delineating the exact functions and contributions each stakeholder brings to the table. By clearly mapping out the participation of various actors in the orchestration of processes and tasks, the CoE's RASCI Matrix ensures seamless collaboration, informed decision-making, and streamlined execution across the spectrum of its LCNC initiatives.

Appendix 1 contains the CoE Governance Framework RASCI Matrix.

5. Monitor and Control

The CoE Governance Framework's monitor and control mechanisms play a pivotal role in ensuring the effective oversight and management of the CoE's operations. Through these mechanisms, the framework establishes a systematic approach to tracking the progress of LCNC initiatives and ensuring their alignment with organizational goals.

The monitor and control processes involve continuous assessment of key performance indicators (KPIs) related to LCNC adoption, project quality, and stakeholder satisfaction. This involves regular data collection, analysis, and reporting to gauge the success of the CoE's efforts. If any deviations or issues arise, the framework guides corrective actions, allowing the CoE to address challenges promptly and make necessary adjustments to keep initiatives on track. By employing robust monitoring and control practices, the CoE Governance Framework empowers the organization to achieve optimal results from its LCNC endeavors while maintaining a proactive stance in managing potential risks and opportunities.

Appendix 2 provides metrics recommended for each identified service management practice.

6. Risk Management

The CoE Governance Framework's risk management component is a strategic process designed to identify, assess, mitigate, and monitor potential uncertainties related to Power Platform. Risk Management is a Governance element embedded in each management practice. General risk guidelines are provided to practice owners. The CoE will provide oversight to ensure appropriate risk management and mitigation.

Methods to Measure Performance

Once established, the Governance Committee can utilize a variety of metrics to measure the performance of its efforts across various key areas.

Adoption Rate: The Governance Committee will closely monitor the adoption rate of LCNC practices and tools across state agencies. By tracking the number of projects, applications, and processes that transitioned to LCNC platforms compared to traditional methods, the Committee can gain insights into the successful uptake of LCNC solutions. A steady increase in adoption demonstrates the appeal and relevance of LCNC tools, driving efficiency and agility.

Quality of Deliverables: The Governance Committee will also place a high emphasis on the quality of deliverables produced through LCNC tools. By systematically evaluating factors such as user satisfaction, application performance, reliability, and adherence to organizational standards, the Committee can gauge the effectiveness of LCNC implementations. Higher user satisfaction ratings and consistently reliable applications will demonstrate the Committee's commitment to ensuring that LCNC solutions meet or exceed IOT's quality benchmarks.

Skill Development: The Governance Committee recognizes the importance of skill development in its LCNC journey. By tracking the improvement in skills and capabilities of resources using LCNC tools, the Committee can observe accelerated learning curves and enhanced proficiency. This directly translates to increased productivity and problem-solving capacity among team members, contributing to the overall success of LCNC projects.

Stakeholder Satisfaction: The Governance Committee will actively seek feedback from stakeholders, including state agency business units, IT teams, and end-users. Through this engagement, the Committee measures stakeholder satisfaction with LCNC outcomes. Positive feedback highlights the alignment of LCNC initiatives with organizational needs, demonstrating the Committee's ability to deliver solutions that resonate with stakeholders' expectations.

By focusing on these critical dimensions, the Committee not only can demonstrate the value of LCNC initiatives, but can also showcase its dedication to driving innovation, efficiency, and growth.

Appendices

Appendix 1 - CoE Governance RASCI

Activities	CoE Sponsor	CoE Chairman	CoE Analyst	IOT Team members	Agency Team members	Technology Partners and Stakeholder
LCNC – Agency Strategy alignment	R	A	S	C	S	I
Establish and maintain a clear vision, mission, goals, and objectives.	A	R	C	C	C	I
Define and maintain governance strategies, architectures, and plans.	A	R	C	C	C	I
Collaborate in LCNC governance	S	A	R	R	R	C,I
Spearhead adoption of CoE Governance and Delivery Frameworks	S	A	R	R	R	C,I
Steer LCNC Road Map - Baseline capabilities & next milestones	C	A,R	S	S	S	C,I
Marketing campaign to communicate successes and opportunities	C	A,R	S	S	S	C,I
Training and upskilling strategy	S	A	R	R	R	C,I
Identify opportunities to fully leverage the true potential of LCNC	C	A,R	S	S	S	C,I
Organizational Change Management	C	A,R	C	C	C	I
Monitor KPIs, LCNC Adoption and Compliance Reports	I	A,R	C	C	C	I
Ensure process effectiveness, efficiency, adaptability, and continuous improvement.	C	A,R	R	C	C	C,I
Determine centralized and decentralized LCNC responsibilities (i.e., recommended SDLC)	C	A	R	R	R	I
Establish governance measurements, implement tracking processes, and distribute governance reports	C	A,R	R	C	C	I

Responsible	Does the work to complete the deliverable or task. Answers to the person Accountable.
Accountable	Answers to the correct and thorough completion of the deliverable or task. Provides formal approval of work completed by those Responsible.
Support	Seeks information to understand problems, expectations, and needs of clients in assigned area. Provides accurate and timely guidance, while also providing resolution-based information when identifying problems and recommending solutions.
Consulted	Sought for opinions on the deliverable or task via two-way communications.
Informed	Updated on progress of the deliverable or task via one-way communication.

Appendix 2 - Management Practices

MANAGEMENT PRACTICE	Knowledge Management

DESCRIPTION

Knowledge Management (KM) is the process of generating, storing, sharing, managing, and effectively using information. KM aims to encourage the access and use of all types of knowledge resources, including databases, documents, policies, procedures, and people's expertise in a collaborative and consumable way to improve people's ability to use information and knowledge effectively and conveniently.

PURPOSE

The IOT CoE Microsoft LCNC portal will create a knowledge base to share Power Platform information with goals to:
• Expand agency awareness of the potential benefits of Microsoft Power Platform LCNC development
• Creation of a knowledge sharing strategy to access information faster and promote LCNC development adoption and co-creation
• Facilitate knowledge and solution exchange between agencies and the LCNC Community of Practice
• "Silo-Busting"
• Reduce knowledge gaps and time to proficiency with access to training links and videos

GOVERNANCE POLICIES and STANDARDS

COE:
• Ensures continuity and distribution of governance policies and standards
• Standardization with reusable assets and templates
• Policies library to maintain standards and improve consistency
• Improve process compliance by including governance in documentation

Information Governance:
• Maintenance of knowledge base content
• Knowledge ownership
• Structured processes for content management
• Track usage

METRICS

• Feedback: Are users able to find information quickly? Do users find the information useful?
• Questions asked per month on a Q&A/discussion forum
• Answers per question on a Q&A/discussion forum
• Portal traffic stats. Number of users accessing portal information. Frequency of visit. Articles viewed, etc.
• Contribution of "managed knowledge" contributed to the LCNC targets

MANAGEMENT PRACTICE	Portfolio Management

DESCRIPTION

Portfolio management is the framework, functions, and processes that guide management activities to optimize investments, deliver business value and create a unique product, service, or result to meet organizational strategic and operational goals. It creates centralized visibility of assets and initiatives with an emphasis on a return on IT investments and focus on the appropriate use of resources to meet organizational strategic and operational goals.

PURPOSE

Portfolio governance activities provide guidance, decision making, and management oversight, whereas the portfolio management activities are specific to organizing and doing the work.

GOVERNANCE POLICIES and STANDARDS

OVERSIGHT function provides guidance, direction, and leadership.	CONTROL function provides monitoring, measuring, & reporting.	INTEGRATION function provides strategic alignment.	DECISION-MAKING function provides structure & delegates authority.
• Analyze portfolio performance results • Establish risk, control & reporting processes	• Portfolio review and audits • Demand Management • Resource and capacity management • Monitor benefit realization	• Align governance Frameworks across agencies • Align project mix and roadmaps • Communicate integrated roadmap	•Determine portfolio and intake prioritization criteria and funding • Perform Go / No Go decisions • Resolve risks and issues

METRICS

• Portfolio Statistics:
  » Total Number of Project Completed / WIP
  » Total Number of Apps Competed / WIP / Retired
  » Total Number of Makers
  » Types of projects by power platform product

• Benefits Realization / Business Value: ROI, NPV, PP, IRR
  » Number of app / projects meeting business case
  » Project success rate
  » Costs

MANAGEMENT PRACTICE	Demand Management

DESCRIPTION

Work Intake (also known as demand management) is perhaps the most critical component of project portfolio management because it determines the composition of the portfolio (in terms of quality, value, balance, and resource utilization). Effective demand management relies on a dependably applied, company-standard methodology. The Intake review and approval process should:
  • be designed with built-in gates to reject or defer projects as soon as sufficient due diligence is completed
  • distinguish different tiers of projects to triage projects that are simpler, shorter, and less risky from the larger projects that need more scrutiny.
 Utilizing the same review process for all types of projects often results in an unnecessarily burdensome process for smaller projects and will be viewed as bureaucratic. Utilizing at least two project tiers allows the lower tier to be a 'fast track' process for smaller, lower risk and less complex projects. This will greatly improve organizational change management and help the company successfully adopt the intake (demand management) process.

PURPOSE

The primary goal of Demand Management is to maximize the strategic alignment and business value of the portfolio, minimize the number of requests rejected or delayed and improve customer satisfaction.

GOVERNANCE POLICIES and STANDARDS

• Establishes a single-entry point for Microsoft LCNC requests and review enabling more consistent project standardization.
• Provides decision-makers an established, standardized forum to examine stakeholder request use case, execution track, project and platform resources, and license requirements.
• Coordination of review and recommendation between CoE and agency.
• Tiered governance for Fast track projects.
• Monitor the allocation of portfolio capacity to different categories of projects – strategic, enhancement, mandatory, and maintenance.

METRICS

• % of project requests accepted by agency, use case, power platform product.
• % of project requests rejected by agency, use case, and power platform product and reason for rejection.
• % of project requests deferred and logged in Master MSFT LCNC project backlog.
• % of project requests referred to existing application for agency review.
• % of project requests referred for collaboration with another agency planning or building a similar application.
• # of project identified by tenant admins not submitted to CoE by agency, use case, power platform product.

MANAGEMENT PRACTICE	Workforce and Talent Management

DESCRIPTION

Workforce and Talent Management encompasses workforce planning, employee engagement, learning and development, performance management, recruiting,
onboarding, succession, and retention. While workforce management concentrates on human resources delivering services, talent management ensures you
have the right people with the right skills – i.e., capabilities – for now and the future. Talent Management focuses on bringing out the best in the workforce
and identifying the career paths and skills employees need to build capabilities.

PURPOSE

Talent Management exists to ensure that organizations get the right people with the right skills into the right position at the right time:
• Ready workforce: Positioned to accomplish evolving priorities and objectives.
• Employee investment: Investment in employees through formal and informal learning and development related activities to close competency gaps and
enhance mission related outcomes.
• Efficient operation: Workforce is aligned, positioned, and trained to provide efficient and effective services to the internal and external stakeholders.
• Increased retention: Retention strategies create committed and empowered employees.
• Accelerated automation: Learning and development activities increases service delivery.
• Trusted labor/management relationship to ensure the workforce has the tools, resources and training to meet business objectives.

GOVERNANCE POLICIES and STANDARDS

• Plan for and manage current and future LCNC workforce needs.
• Design, develop, and implement proven strategies and techniques and practices to attract, hire, develop, and retain talent.
• Close LCNC knowledge, skill, and competency gaps throughout the agencies.

METRICS

• Workforce Planning: % of critical staffing gaps closed
• Recruitment and Outreach: % of reduction in time-to-hire
• Employee Development: % of employee that participate in training; % of employee certified by role; time to full productivity / FTE
• Leadership Development: % of technical leadership staffing gaps closed

MANAGEMENT PRACTICE	Business Analysis

DESCRIPTION

Business analysis as a management practice means that organizations can more effectively communicate their requirements. It is one of the seven stages of all
SDLC methodologies.
• Analyzing business systems or problems, processes, architectures, and services.
• Identifying and prioritizing parts of an outcome or service that need improvement as well as capturing opportunities for innovation.
• Evaluating and suggesting solutions that will meet both current and future business needs.
• Documenting business requirements in a structured way.
• Recommending solutions after reviewing and validating the requirements with the appropriate stakeholders.

PURPOSE

Business Analysis Governance is the Framework that governs and guides a project's entire business analysis process. It sets the rules, principles, and guidelines for conducting business analysis activities to achieve project objectives.

GOVERNANCE POLICIES and STANDARDS

• Establish transparency, accountability, and consistency in decision-making processes throughout the project lifecycle.
• Provide a structured approach for managing requirements, identifying risks and constraints, and aligning stakeholders' expectations.
• Establish communication channels between stakeholders
• Implement change management protocols
• Ensure compliance with industry standards or regulatory requirements.

METRICS

• Difference between ROI and NPV in the planned baseline and the actual
   ROI and NPV.
• Increase in productivity after implementing solution.
• Reduction in cycle time after implementing solution.
• Decrease in cost attributed to solution.
• Percentage of rework attributable to requirements.

• Percentage of projects with prioritized requirements.
• Percentage of requirements fully implemented.
• Overall developer satisfaction with requirements.
• Overall QA satisfaction with requirements.
• Number of iterations of requirements revision.
• Number of missed requirements/miscommunicated requirements.

MANAGEMENT PRACTICE	Software Development and Management

DESCRIPTION

The purpose of the software development and management practice is to ensure that applications meet internal and external stakeholder needs, in terms of functionality, reliability, maintainability, compliance, and auditability. The seven phases of software development and management are:

• Planning
• Requirements
• Business Analysis
• Architecture and design (user interface, CX, service design, etc.)
• Development (Build)

• Test (which can include several components, such as unit testing, integration testing, regression testing, information security testing, and user acceptance testing)
• Deployment

PURPOSE

Software Development and Management governance ensures that a software development project meets customers specifications and aligns with business goals and complies with external regulations. It establishes a formal Framework for achieving measurable progress toward project objectives while maintaining compliance standards, protecting data security, supporting data retention, and ensuring disaster recovery. An operating model oriented to LCNC development provides a complementary governance structure to address requirements around suitability, scalability, supportability, security, and accessibility of applications built on the power platform.

GOVERNANCE POLICIES and STANDARDS

• ALM environment management / No development or testing in production.
• SDLC management of functional and technical (non-functional)l requirements
• Sufficient application and integration documents for support personnel and/or a new maker
• Power Platform Security policies / Least privilege policies.
• Software development fundamentals: training around security, data protection, version control, and systems integration.
• Project, Risk and Change Management

METRICS

• Number of applications in development
• Number of live applications
• Number of platform logins (by citizen developers)
• Number of integrations with other applications
• Number of reusable pieces/components used
• Number of active citizen developers
• Number of users of citizen development-built applications
• Number of business processes that use citizen development

• Average time to market of citizen development applications
• Average time to ideate
• Average time to build/deploy
• Average time to value delivery
• Average time to change application
• Average time to repair defects
• Number of projects going down fast track versus assisted path
• Number of projects returning to fast track after detailed assessment

MANAGEMENT PRACTICE	Deployment Management

DESCRIPTION

Deployment management is the migration and deployment of software code, configurations, or content between development, test, and production environments. Effective software deployment is critical for ensuring that software applications are delivered securely, reliably, and efficiently

PURPOSE

Deployment Management Governance ensures that software is configured, tested, released, and installed in a consistent and controlled manner. It is related to Configuration Management, Change Control and Quality Assurance to establish the necessary controls that allow deployments to be managed and monitored throughout the application lifecycle.

An important part of IT asset management is applying process across all lifecycle stages to understand the total cost of ownership and optimize the use of assets.

• Automate the deployment process (CI/CD) to save time, reduce errors, and improve the overall efficiency of the process.
• Use version control to manage changes to the software application and ensure that the correct version is deployed.
• Conduct thorough testing to ensure the software application is functioning correctly and meets the requirements of the end-users.
• Deploy in phases to reduce risk and ensure successful deployment.
• Monitor post release application performance to ensure that it is functioning correctly.

METRICS

• Deployment Cycle Time
• Deployment frequency
• Application Availability
• % Change in number of incidents for unsuccessful software releases

• % of deployment roll backs
• % Reduction of implementation and maintenance costs
• MTTR of deployment tickets

MANAGEMENT PRACTICE	Asset Management

There are two main PSF (Practice Success Factor) in the practice:
ensuring that the organization has relevant information about its IT assets throughout its lifecycle,
ensuring that the utilization of IT assets is continually monitored and optimized.

IT asset management (also known as ITAM) is the process of ensuring an organization's assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes. Assets include hardware, software, cloud-based assets, licenses, subscriptions, and contracts. Asset Management is the foundation for multiple management practices to include Change Management, Problem and Incident Management and Configuration management.

PURPOSE

Asset management governance defines standards and operating procedures for asset tracking, documentation and utilization and coordinates data capture across multiple departments.

GOVERNANCE POLICIES and STANDARDS

• Consistent monitoring procedures to ensure all relevant assets are accounted for.
• Maintain current LCNC application, infrastructure and license inventories of tangible and intangible assets to reduce waste and improve utilization.
• Performs scheduled asset audits to verify inventory information.
• Executes control processes to enforce compliance with security and legal policies.
• Manages consumption of "on-demand services."

METRICS

• Asset Utilization
• Asset Availability
• Schedule Compliance
• Servicing and Maintenance schedules
• % of virtualized assets under control / not under control
• Audit History

• # of assets being managed by asset type (HW, SW, etc.)
• # of software licenses being managed
• # of installed software instances being managed
• # of purchased licenses
• # of assets maintained by external partner(s)
• # of unauthorized and/or non-corporate assets

MANAGEMENT PRACTICE   Incident Management

DESCRIPTION

Incident management is the process of managing IT service disruptions and restoring services. The quick restoration of a service is a key factor in user as well as customer satisfaction, the credibility of the provider and the value organization creates in the service relationships. Incident Management processes include:
• Incident Detection and Recording.
• Incident Classification and Support.
• Incident Investigation and Diagnosis.
• Incident Resolution and Recovery.
• Confirmation and Closure.

PURPOSE

The purpose of incident management practice is to minimize the negative impact of incidents by restoring normal service operation as quickly as possible in a controlled and predictable manner. The CoE will not provide direct incident management support to Power Platform applications and infrastructure but rely on the existing incident management process of the end-user agency; unless the application is supported by the IOT LCNC team, in which case the current ASM ticketing system will be utilized. The CoE will aggregate enterprise incident statistics to refine governance and management practices.

GOVERNANCE POLICIES and STANDARDS

Incident management governance establishes practices and procedure guidelines to respond to incidents and mitigate future incidents. Once incidents are identified and mitigated, knowledge of those incidents and necessary responses can be applied to future incidents for faster resolution or all-around prevention.

METRICS

• # of Incidents over time
• MTTA
• MTTR
• Avg Incident Response Time
• First Touch Resolution Rate
• On-Call Time
• Escalation Rate
• SLA
• Cost / Incident
• Uptime

MANAGEMENT PRACTICE	Risk Management

DESCRIPTION

Risk management is the process of identifying, assessing, and controlling financial, legal, strategic and security risks to an organization's tangible and intangible assets.

PURPOSE

To fully benefit from no-code/low code technology, IOT must enable people outside of IT. This introduces risks—security, data protection, storage, systems integration, version control, and so on—that are vital considerations for any organization. To seek further adoption, organizations must create a controlled and secure technical environment with accepted protocols that can be applied by departments in the organization and governed by IT.

GOVERNANCE POLICIES and STANDARDS

Security
• Protection of confidentiality, data loss, & uncontrolled user access.
Operational IT
• Establish applicable policies, standards & rules to create, manage, maintain
  & use IT
IT Architecture
• Establish rules to build, modify and interface IT resources

Regulatory
• Monitor external laws, industry standards or compliance requirements.
Reputational
• Prevent negative perception of services by legislators and citizens
Financial
• Monitor service budgets and equipment expenditures.

METRICS

• # of risks identified
• # of risks that occurred (became events)
• Predicted risk severity versus actual risk severity
• # of risks that were not identified
• Cost of risk management

• # of risks that occurred more than once
• # of risks closed
• % of risks monitored
• # of risks mitigated
• % of agencies involved in risk assessment

MANAGEMENT PRACTICE	Power Platform Management

DESCRIPTION

Power Platform Admins are responsible for monitoring key metrics in the CoE Toolkit and ensuring general environment hygiene is addressed in a suitable cadence. The are also responsible for following and ensuring best practices are being followed within the Platform.

PURPOSE

Establish a Center of Excellence (CoE) to provide platform governance, design patterns and practices, and advanced end-user training. The CoE governance model places the design, development, and support of the products in the hands of experienced managers and end-users.

GOVERNANCE POLICIES and STANDARDS

SECURITY	MONITORING	ENVIRONMENT	EDUCATION
• Ensure Power Platform Admins are creating necessary global DLP Policies.	• Assign the appropriate monitoring tasks to Power Platform Admins • Identify monitoring frequency	• Favor Decentralized vs centralized management • Ensure Platform Admins are following proper Environment hygiene	• Ensuring Admins and Makers are educated • Promote the use of the Power Platform

METRICS

Hygiene
Identify Orphaned apps and flows
Identify Non personal productivity Apps and flows in default environment
Identify Incorrect use of core connectors
Identify Use of Environment Level DLP policies
Identify Utilization of Correct License Type for Use Case
Identify Where there 2 Agency Admins assigned for each app/flow