Guiding Principles/Roles and Responsibilities
Information Technology Governance

Information technology (IT) governance is a subset discipline of corporate governance which focuses on information technology and its alignment with business objectives and effective risk management practices. The purpose of IT governance is to: align IT investments and priorities with the organization's strategy and goals, prioritize and manage requests for IT services that optimize returns to the organization, manage major risks and threats proactively, ensure responsible utilization of resources and assets, and improve IT organizational performance.

The Credit Union Prudential Supervisors Association (CUPSA) is providing this guidance to help institutions better understand effective IT governance oversight principles and appropriate roles and responsibilities. The principles and practices outlined in this guidance are intended to be scalable to the relative size, scope, complexity and risk profile of an institution, and are consistent with the IT governance principles established by the IT Governance Institute (ITGI).

Guiding Principle 1 - Strategic Alignment

Strategic alignment ensures that IT initiatives and standards support the institution's strategy and goals. This involves:

- Obtaining support for IT from executive management;
- Understanding the needs of the business; and
- Developing IT strategy and objectives.

Common practices could include:

- Ensuring that IT is included in the strategic planning process;
- Aligning IT strategy with corporate objectives; and
- The existence of IT steering committee.

Guiding Principle 2 - Value Delivery

Value delivery ensures that value is obtained from investment in IT by selecting investments wisely and managing them throughout their life cycle. Effective value delivery ensures that IT initiatives are completed on-time, on-budget and meet expectations. This involves:

- Identifying project drivers and goals;
- Identifying service delivery drivers and goals;
- Overseeing project management and delivery goals; and
- Facilitating communication of the value of information technology.

Common practices could include:

- Effective requirements gathering;
- Communication plans for new initiatives;
- IT project tracking and reporting;
- IT projects meet stated objectives; and

- Benefits realization phase included with project close out procedures.

Guiding Principle 3 - Risk Management

Risk management ensures the safeguarding of IT assets, disaster recovery and continuity of operations including security and information integrity. This involves:

- Setting the institutional risk appetite, with respect to IT;
- Determining information security and IT risk management strategies;
- Monitoring application of IT risk management strategies;
- Understanding compliance and regulatory mandates;
- Ensuring information is managed through effective quality control practices; and
- Collaborating with IT audit functions and supervisors.

Common practices could include:

- Established change control procedures;
- Defined IT risk appetite and risk and mitigation strategies incorporated into institution's enterprise risk management framework;
- Regulatory compliance processes;
- Existence of a data governance framework;
- Information classification policies (types of data, and levels of access);
- Business impact analysis documentation;
- Information security management processes (privacy, classification, etc.); and
- Established business continuity planning/disaster recovery planning, incident management and escalation procedures.

Guiding Principle 4 - Resource Management

Resource management examines the optimization of IT resource use and allocation and how the institution manages and delivers critical IT resources. This involves:

- Overseeing resource allocation and portfolio management;
- Managing hardware and software assets;
- Maintaining third party service providers and outsourced arrangements; and
- Enforcing standardized architecture standards.

Common practices could include:

- Adequate internal IT staff or outsourced arrangements;
- Service delivery processes;
- Resource allocation and planning;
- IT operating and capital budgets;
- IT asset management protocols;
- Service-level agreements (SLAs) with all third party vendors; and
- Confirmation reports from third party service providers.

Guiding Principle 5 - Performance Management

Performance management examines how IT staff track and monitor their IT implementation strategy, how the success of projects is determined, and whether a high level of service delivery has been maintained. This involves:

- Ensuring customer satisfaction;
- Maintaining expected service levels;
- Measuring business value on service delivery; and
- Fostering IT process improvement initiatives.

Common practices could include:

- IT performance management metrics;
- IT performance reports;
- List of identified processes with proposed improvements; and
- Inclusion of performance management effectiveness in audit scope.

IT Governance Roles and Responsibilities

A sound understanding of appropriate roles and responsibilities is essential to an effective IT governance framework. CUPSA has identified key roles and responsibilities as follows:

Board of Directors

- Reviewing and approving an IT governance strategy and policies around the effective use of information technology;
- Overseeing progress reporting on strategic initiatives;
- Evaluating and monitoring the alignment and decision making process between corporate objectives and information technology priorities; and
- Ensuring that IT governance is included within the internal control framework.

Senior Management

- Planning, prioritizing and organizing IT initiatives and allocating appropriate budgets within the institution;
- Directing resources toward information technology initiatives;
- Providing reports on the performance, effectiveness and security of the information technology infrastructure to the board; and
- Providing progress reporting on major strategic IT initiatives (e.g. migrations between banking systems, new products, etc.) to the board.

External/Internal Audit

- Evaluating the system's internal control design and effectiveness; and
- Confirming that IT infrastructure is safeguarding assets, maintaining data integrity and operating effectively to achieve the organization's goals or objectives.

Third Party Service Providers

- Reporting to institutions to confirm that hosted and outsourced products have been properly audited and assessed.

Regulators

- Providing standards of sound business practices for IT governance and risk management;
- Assessing institutions' adherence to standards of sound business practices around IT governance and risk management; and
- Taking appropriate supervisory action and working with institutions to ensure that sound IT governance practices are implemented.