
NBIM Policy – Information Technology (IT)

Issued by: Chief Executive Officer, Norges Bank Investment Management
Effective date: 20/03/2012
Last updated: 20/06/2012

1 Purpose

This policy defines principles for delivery of information through systems, services and technology. The objective is to ensure a common set of principles, requirements and expectations that apply to govern the information technology capabilities of the organisation and the relationship between consumers and providers of such capabilities.

2 Scope

Information Technology (IT) is in this document referred to as data, systems, services and technologies that together provides NBIM with information, electronic communication and business process execution capabilities. The principles laid down here shall as far as possible also apply where information technology services are provided directly from external suppliers.

This policy is based on the COBIT¹ good practice framework for information and technology governance, adapted to NBIM's operational model for IT services. It is divided in four main IT governance areas:

- Plan and organise;
- Acquire and implement;
- Deliver and support;
- Monitor and evaluate.

The following definitions apply:

Solution - shared term covering information systems and services that together form capabilities to perform a set of related business processes.

NBIM infrastructure – infrastructure hosted by NBIM, NBIM's main infrastructure provider or an Application Service Provider (ASP).

Service desk – single point of contact for end user requests.

3 Policy

Information technology shall enable efficient execution of business processes and distribution of information. The following main principles apply:

- NBIM shall seek simplicity and integrity of solutions.
- NBIM shall measure the quality and service levels of existing solutions to allow continuous improvement.

¹ COBIT is a framework for information technology management and IT governance established by ISACA – independent global association providing knowledge and practices for information systems.

4 Plan and organise

This area addresses strategy and tactics, and concerns the identification of how information technology can best contribute to the achievement of NBIM's objectives. It also links strategy and planning with continuous improvement of processes, and it describes the current state of information technology processes, organisation and structure.

4.1 Strategy and technology direction

The information technology strategy shall describe strategic objectives, tactical plans and direction for information technology, systems and services. It shall also provide an evaluation of current information technology risks, performance and contribution.

- The information technology strategy shall have its foundation in NBIM's strategy plan.
- Technology direction shall ensure standardisation and consolidation of solutions and technologies.

4.2 Architecture

Information architecture, solution architecture and technology architecture are part of the NBIM Governance Model.

- An overview of the current state architecture shall be available at all times.
- Architecture compliance for new and existing solutions and technology shall be defined through principles with a foundation in this policy, strategy and technology direction.

4.3 IT processes

IT processes, quality assurance, organisation and relationships are defined as part of the NBIM Governance Model. Assessment and handling of operational risk is governed on an NBIM level, across IT and other processes, in accordance with the NBIM Policy – Operational risk management.

4.4 Project portfolio management

Major changes to architecture and solutions shall be implemented through projects. All projects shall have a foundation in NBIM's strategy plan.

Governance and the management of projects should be in accordance with the NBIM Guideline – Project management methodology.

5 Acquire and implement

To realise NBIM strategy, IT solutions need to be identified, acquired or developed.

Identification and procurement shall follow general procurement rules in accordance with the NBIM Policy – Procurement, and adhere to public procurement rules and regulations. Normally, larger procurements and development efforts will be handled as projects.

- Business requirements and business case evaluation shall be the basis of acquiring or developing solutions.
- Technology choices shall be based on solution requirements and technology direction.
- NBIM has a preference to purchase commercial off the shelf solutions or services over building these ourselves.
- Systems development and maintenance shall follow defined development and coding standards.

5.1 IT change management

All changes, including emergency maintenance and patches related to infrastructure and solutions within the production environment shall be managed through a change management process. This process shall cover release and deployment, change, configuration, validation and testing as well as change evaluation.

- All changes shall be specified and designed in accordance with architecture principles.
- Changes shall be subject to testing and verification prior to release in production environments.

6 Deliver and support

Delivery includes service level management, security and continuity, end-user support, data management, IT operations and systems management.

6.1 Service level management

Service level management contains processes for creating service requirements and defining services and service level agreements. It sets expectations for management of information systems, services, data and supporting technology.

- An overview of services and solutions shall be maintained. The overview shall include service definitions, service levels, Key Performance indicators (KPIs), criticality classification, service owner and responsible.
- Services shall be cost efficient. A cost picture including financial costs, internal costs and operational risks shall be maintained for all services.
- Services shall be evaluated regularly to identify areas of improvement.

6.1.1 IT operations

IT operations is a collection of processes related to scheduled processing, performance and capacity monitoring, physical environment management and preventive infrastructure maintenance.

- Service levels shall be agreed for technical infrastructure based on the criticality of dependent solutions.
- Procedures to ensure timely maintenance of NBIM infrastructure shall be in place.

6.1.2 Systems management

Systems management is the practice of management of system providers, service levels, solution configuration and end-user training and expectations.

- All systems shall have a system owner which represents the area drawing benefits from the system.
- All systems shall have a system manager who supports the system owner as required, and ensures that necessary support, change, control and training processes are in place.
- Provider management shall follow general rules in accordance with the NBIM Policy – Service Provider Arrangements.

6.1.3 Data management

Data management considers processes to ensure quality, consistency and availability of data.

- NBIM shall perform cost-efficient provisioning of data.
- NBIM shall maintain consistency of data across solutions.
- Management of data shall be prioritised according to business value and materiality.
- Data and information elements shall be defined and classified in a central repository.

6.1.4 Service desk

NBIM shall have a timely and effective process to handle incidents and service requests. This shall include problem management in order to identify and address root causes for incidents which will ensure continuous service improvement for the organisation.

- All incidents, service requests and change requests shall be managed by the service desk as a single point of contact.
- Service desk shall be available to all NBIM locations during working hours.
- End user shall receive confirmation of incident and service request retrieval, with set priority and expected resolution time.

6.2 IT security and business continuity

IT security and business continuity shall ensure integrity of information and protect NBIM's information and infrastructure in order to minimise the business impact of security vulnerabilities and incidents. The NBIM Policy – Information Management describes the principles and requirements for information security. Disaster recovery for information systems and services shall follow principles in accordance with the the NBIM Policy – Business continuity management.

- IT security measures shall take into account security classification of the solutions and data to be protected.
- IT disaster recovery procedures shall be established and tested on a regular basis.

7 Monitor and evaluate

All information technology processes shall be assessed for quality and compliance with control requirements.

7.1 Reporting

Reporting shall ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with requirements. The purpose of reporting is to identify and implement performance improvement actions.

- Reporting shall be based on agreed upon targets for processes and performance.
- Reporting shall be balanced between service level improvement opportunity and reporting effort.

7.2 Internal control

Principles for internal control shall be in accordance with the NBIM Policy – Operational risk management.

7.3 Investment Architecture model

The NBIM Investment Architecture model is part of the overall NBIM governance model described in the NBIM Governance Model.