Universitas Komputer Indonesia

Chap 9 Management, Planning, and Organization of Information Systems

Dr. Ir. Yeffry Handoko Putra, M.T

Magister Sistem Informasi
Universitas Komputer Indonesia

IF 37325P

Content

1. Evaluate the IS Strategy and Alignment with the Business Objectives
2. Evaluate the IS Organizational Structure
3. Evaluating IS Policies, Standards, and Procedures
4. Evaluating Problem Management
5. Evaluating Third-Party Services Selection and Management
6. Evaluating Project Management
7. Evaluating Change Management
8. Evaluating Quality Management
9. Evaluating Performance Management

Evaluate the IS Strategy and Alignment with the Business Objectives

- Knowing the vision of the business owners and decision makers
- gather about the company direction, culture, or long-range plans willbe helpful for developing value-added audit strategies
- You will need to determine what that guidance is when it exists in a documented form.
- You may investigate annual reports for such information or find it on Web pages or corporate literature
- You may investigate annual reports for such information or find it on Web pages or corporate literature

Evaluate the IS Strategy and Alignment with the Business Objectives

Systems Architecture

The model should be kept current, be well documented, and be maintained for accuracy and completeness as changes occur and the direction evolves

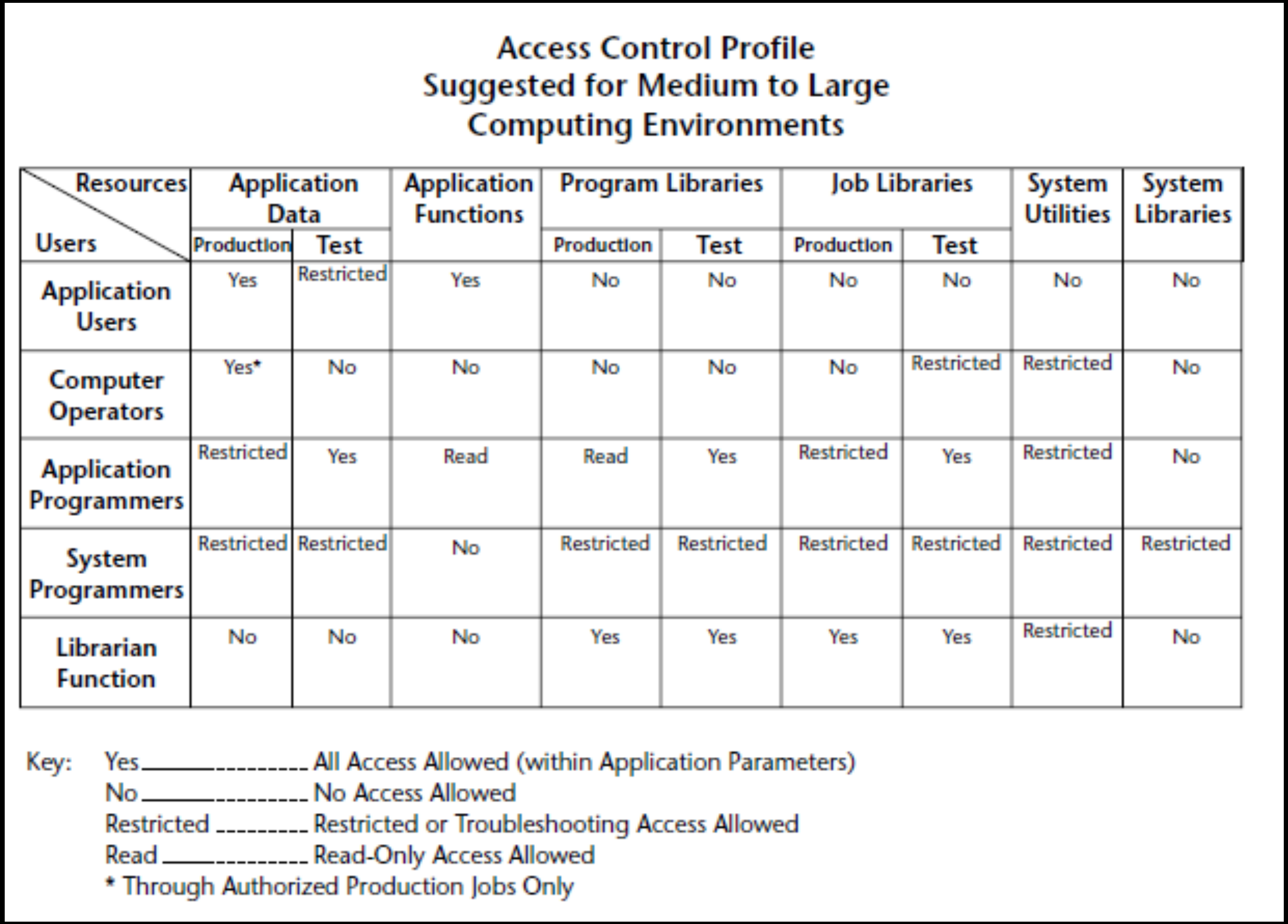
Evaluate the IS Organizational Structure

- Roles and Responsibilities
  - Segregation of duties
- Database Administration

  - Specifying data definitions
  - Preparing programs to create data
  - Sizing tables and storage requirements for database systems
  - Testing and evaluating queries and table joins
  - Implementing access controls, update controls, and concurrence controls
  - Performing database optimization and tuning
  - Monitoring database and space usage
  - Defining and initiating database back up and recovery procedures

Evaluate the IS Organizational Structure

- Qualification and Training of the IS Staff Staffing practices



Access Control Profile
Suggested for Medium to Large
Computing Environments

Resources / Users	Application Data		Application Functions	Program Libraries		Job Libraries		System Utilities	System Libraries
	Production	Test		Production	Test	Production	Test		
Application Users	Yes	Restricted	Yes	No	No	No	No	No	No
Computer Operators	Yes*	No	No	No	No	No	Restricted	Restricted	No
Application Programmers	Restricted	Yes	Read	Read	Yes	Restricted	Yes	Restricted	No
System Programmers	Restricted	Restricted	No	Restricted	Restricted	Restricted	Restricted	Restricted	Restricted
Librarian Function	No	No	No	Yes	Yes	Yes	Yes	Restricted	No

Key: Yes ________________ All Access Allowed (within Application Parameters)
No ________________ No Access Allowed
Restricted __________ Restricted or Troubleshooting Access Allowed
Read ______________ Read-Only Access Allowed
* Through Authorized Production Jobs Only

Evaluating IS Policies, Standards, and Procedures

- Policy
  - ○ Ethics, values, integrity, and principles
    - – Mission and vision of the entire organization
    - - ManagementÕs philosophy and style
    - - Quality and service commitments
    - - The accountability and direction provided by the board of directors
  - – Responsibility and accountability for the protection of the shareholders
  - – Õ assets and business goals
  - - Operational style and business segment direction
  - - Legal and regulatory commitments
  - - Overarching directives related to control, security, financial, or
  - – human resource framework issues

Evaluating IS Policies, Standards, and Procedures

- The majority of topics covered in IS policy
  - High-level security policy evidencing authority and responsibilities
  - Disaster recovery and business continuity planning
  - Ethical behavior and acceptable use
  - Service commitment and management
  - Data valuation and classification
  - Data protection and disposal
  - Information ownership and its related roles and responsibilities
  - Access control and authorization
  - Internet security, data protection, and virus protection as appropriate
  - Email use, expectation of privacy, and data ownership position
  - Intellectual property rights, copy protection, data transfer, and so forth
  - Operations and system
  - systems responsibility
  - Problem management
  - Change management
  - Data and network management
  - Security awareness and user obligations issues
  - Training and human resource policy
  - Security incident reporting and response
  - Legal and regulatory issues (for example, in healthcareÑnaming a
  - security and privacy officer)

Evaluating IS Policies, Standards, and Procedures

- The documentation format of a policy should include
  - The bright line principle or policy statement
  - Why this principle is needed and where it is applicable-- possibly through a background section
  - Definitions necessary to understand the context of the policy
  - Responsibilities of various members of the organization related to the policy
  - Enforcement authority and consequences for noncompliance
  - Information on where to go for more information, such as related policies, standards, and procedures
  - Who is responsible for maintaining the review of the policy
  - The owner and last review date

Evaluating IS Policies, Standards, and Procedures

- Standards
- Procedures

Evaluating Third-Party Services Selection and Management

- During your review, you should investigate and gather evidence of the following steps
  1. Define the business objectives and requirements.
  2. Identify the necessary technologies for the delivery of the requirements.
  3. 3. Perform a baseline risk assessment, analyze the rational, and document the business decision.
  4. Specify delivery and control requirements based on the entire business process flow.
  5. Perform due diligence in selecting potential vendors, validating control, and accessing delivery abilities.
  6. Define contractual, service-level, and insurance agreements.
  7. Document procedures, responsibilities, controls, and monitoring mechanisms.
  8. Execute an agreement and plan transition implementation.
  9. Perform an ongoing relationship management and monitoring.

Evaluating Third-Party Services Selection and Management

- Contract Management
- Service Level Agreements

Items to consider when reviewing an SLA include

- Scope of work or service performed
- Expectations/definition of normal service
- Processes for handling exceptions and changes to normal service provisioning, restrictions, and so forth
- Costs and charges for the various service levels
- Measurement criteria and reporting commitments against those criteria (frequency, response time, and so forth)
- Definitions of acceptable service deliverables, response times, and processes for addressing customer service support (this might include escalation procedures, penalties, and so forth)
- Continuity and disaster recovery planning, security, legal requirements, and so forth as appropriate
- Process for renegotiating based on the changing situation of either party, such as capacity or growth requirements on changing needs
- Retention and storage of media, logs, and historical information
- Notification processes and commitments for “out of bounds “ conditions

Evaluating Project Management

The detail aspects of each task also will need to be defined:

- How much effort is required to perform each task?
- How many resources are necessary to perform this effort?
- Is there any opportunity for getting the work done faster by applying multiple resources to the task or to work multiple tasks concurrently?
- Are there other tasks that need to be done before this particular task?
- What are the costs associated with the materials and manpower to complete each task?
- What is the estimated time span needed to perform a unit of this task’s type?
- What other steps of the overall objective are waiting for this task to complete before they can begin?

Evaluating Change Management

This gatekeeper has several roles

- Ensures that changes have been approved by process owner
- Ensures that changes have been thoroughly tested for deployment in the live production environment
- Ensures that back-off procedures are available, should the change Fail
- Checks that the impacts of the changes have been considered and communicated to the affected parties
- Ensures that corresponding disaster recovery processes have been updated prior to the implementation of the change
- Determines that the source and object code match when applicable
- Records the change and provides an audit trail of the code movement
- Promotes the change to production in an independent and impartial manner
- Determines the success or failure of the change and initiates the back-off procedure when required

Evaluating Problem Management

- When reviewing the problem management processes, you will be assessing the IS organization’s ability to identify, examine, and resolve problems that occur in the IS environment
- A problem management system should capture and document all events that are not standard operational events.

Evaluating Quality Management

System Development Life Cycle (SDLC)

- A new idea is generated for a system or improvement.
- The idea is preliminarily accepted for potential funding by a sponsor, owner, or user group.
- Problem analysis:
  - The feasibility of the idea is investigated and data is gathered and analyzed related to the cost and benefits, along with other alternative courses of action.
  - Classic problem definition and current state analysis is performed and documented to understand the primary problem that is to be solved using root cause analysis techniques.
  - The constraints of existing and potentially future solutions are identified.
  - The resultant idea feasibility and options for moving forward are documented and presented to the sponsor for approval.

Evaluating Quality Management

System Development Life Cycle (SDLC)

- Solution design:
  - If approved for further study, criteria are developed for a successful implementation and are documented along with the functional requirements for the system to meet the needs of the sponsor and the proposed idea.
  - Processes are defined by system flowcharts and data flow diagrams to better understand the possible solutions and project tasks involved with deploying the various solutions.
  - Various solutions are analyzed, buy versus build analysis is performed, software acquisition strategies are investigated, and inhouse versus contract services are reviewed as options.
  - The technical feasibility of the various solutions is examined and reconciled with the organizations infrastructure, data model, current and planed system architectures, configurations, and so forth.
  - The economic feasibility also is examined of the top choices for solutions and compared to ROIs and the budgeted resources available.
  - Risk analysis of the various options, including security and control concerns, are documented and prepared for the final proposal along with recommendations for risk mitigation.
  - Solution proposals are made with recommendations of the systems development goals, costs, and deliverables expectations for approval by system owner/sponsor

Evaluating Quality Management

System Development Life Cycle (SDLC)

- System design :
  - Based on the approved and agreed upon scope and constraints, the system is designed and developed considering users needs, data requirements, functional and processing requirements, training, interfaces, inputs, outputs, internal and application controls, audit trails, availability, data integrity, security requirements, and reports.
  - Requests for Proposals (RFPs) are designed and submitted as appropriate and contracts are negotiated with various providers and vendors. For contract programmers, a specific contract language ensures that the adequate controls over deliverables, quality, performance to standards, and workmanship, as well as supportability issues exist.

Evaluating Quality Management

System Development Life Cycle (SDLC)

- System design :
  - Project plans are built defining the required resources, timeframes, deliverable milestones, and so forth. This is the point where review criteria is developed and agreed upon to ensure that design goals are met.
  - Mock-ups and a cost-benefit analysis are presented for approval and final sign-off of development by the departments of management and the affected users.

Evaluating Quality Management

System Development Life Cycle (SDLC)

- System development:
  - Equipment is purchased and installed properly.
  - Systems are developed in the test environments.
  - Programming occurs either through internal or contract resources.
  - Several iterations of programming and testing are staged and integrated to achieve the final objectives.
  - The testing staged includes unit testing, integration testing, regression testing, hardware and component testing, load and stress testing, pilot testing, user acceptance testing, performance testing, and total system testing. This testing should have provisions for protecting sensitive data in the testing phases. The testing duties should be segregated from development tasks as much as possible to ensure the fair analysis and testing of the resultant system or programming components

Evaluating Quality Management

System Development Life Cycle (SDLC)

- System development:
  - User screens are developed and tested.
  - Initial systems documentation is produced.
  - Test data is processed for the required objectives testing.
  - Facilities planning and implementation is developed with acceptance procedures defined for all of the environment and support needs.

Evaluating Quality Management

System Development Life Cycle (SDLC)

- System implementation:
  - Based on approval and sign-off, implementation and production deployment is planned.
  - File conversion is performed to populate the final system.
  - Systems conversion is planned and executed using pilot, parallel, or full-system cutover methodologies.
  - User and operations manuals are documented and completed
  - Users and operators are trained.
  - The final cutover is created, involving close interaction and communication with the system users.

Evaluating Quality Management

System Development Life Cycle (SDLC)

- Maintenance and modifications:
  - The system undergoes routine maintenance and bug fixes with scheduled improvements prepared over time using mini-SDLCs.
  - An ongoing, operational use and utilization of system occurs.
  - The periodic assessment of design and performance based on the needs and changes in technologies also occurs.
- Cycle repeats:
  - A new idea is generated for the improved system to better meet
  - the needs of the owner/sponsor of the user group.

Evaluating Quality Management

Quality Assurance Standards and Procedures

- Hardware planning, obsolescence and capacity standards, and purchase procedures
- Proper hardware installation, configuration, and hardening practices
- Test environment establishment, usage, and documentation
- Testing standards, parallel/pilot testing, unit testing, aggregated program testing, stress testing, and the segregation of duties during testing, and so forth
- Code migration, test partitioning, storage, and back up
- Coding and program specifications and documentation techniques
- Naming of conventions and data dictionary standards
- Configuration design requirements and format standards
- Purchasing, bidding, and selecting a vendor
- Maintenance, upgrades, and patch application
- Key performance measurements, and other quality metrics
- Customer communication, report formatting, and so on
- User training and documentation
- Change control and production data migration

Evaluating Performance Management

Key Performance Indicators (KPIs)

- Measures of output quantity, quality, efficiency, timeliness, mean time between failures (MTBF), and service level metrics are all performance indicators that should be recorded and tracked over time.
- Using KPIs, management is able to assess the temperature and health of the organization quickly and drill down to other metrics and reports when alerted by these indicators that something is amiss.

Evaluating Performance Management

Performance Measurement Techniques

- Measurements of the workload, both historically over the past shift day, week, and month, and projected work in the queue to be used in anticipation of peaks and valleys in a demand curve. This is typically captured from shift summary reports or machine counters that are read and recorded on a routine cycle. Often, the data can be gathered automatically from log data or through consoles that are used to monitor throughput and the success or failure of completed procedures or operational tasks.
- Capacity monitoring and measurement of various flavors, including but not limited to, CPU usage and cycles, storage availability, and the use of various media types (DASD, disk, tape, off-site, bandwidth, number of concurrent users, and so on) is an important aspect of the business to keep an eye on
- Customer satisfaction is a good measurement of performance but often a difficult one to get objective data on. satisfaction can be ascertained by monitoring help desk calls or complaints to a complaint line. Keeping track of problems reported, length of time problem remains outstanding, number of outstanding problems, impacts to users from problems in duration, and severity all fit into this category.

Evaluating Performance Management

Performance Measurement Techniques

- The most common measurement is against known deliverables and service levels agreed to in a performance commitment of some kind, such as an SLA. In fact, a primary reason for developing an SLA is to reach agreement on what is measurable, what the benchmarks and standards are for those measurements, and what the action plans are to be should variances occur that are unacceptable to one party or the other.

Evaluating Performance Management

Evaluating Capacity Management

- Capacity management is more than just keeping track of when you are about to run out of disk space, tapes in the library, or exceed a fixed percent utilization of a processor. Good management practices are proactive and seek out changes so they are planned for and anticipated
- Knowing that the capacity planned for will enable you to save money by buying at a time when the market rates are favorable or when a larger unit will give a better price break for the whole years needs, are often significant cost issues in the IT business

Evaluating Performance Management

Economic Performance Practices

- You must evaluate the annual budgeting processes of the IS organization to ensure it is properly funded to perform the tasks it is assigned
- Capacity requirements and associated costs should be budgeted for in the months that the needs are required so that the IS organizations can successfully meet their service agreements.

Expense Monitoring

- The monitoring of expenditures against the planned budget is an important
- control function that should be apparent in your review of the management processes

Evaluating Information Security Management

- The root concerns of information security are identification, authentication, and authorization
- information security management cannot be responsible for the elimination of all security risks

Evaluating Performance Management

The information technology security plan should have several of the following common elements:

- Periodic risk assessments and evaluations of current security status
- Incident identification and response, and follow-up processes
- Policy, standards, and leading practices of identification creation and communication
- Security awareness and training processes
- Communication-related security activities (phone or dial-up, Internet, trading partner connectivity, and so forth)
- Data access control activities, such as information ownership, data classification, firewall management, content control tool administration, and so forth
- User account administration activities including adding users, modifying access needs, terminating accounts, periodically revalidating access needs, resetting password, and managing accounts and data access pairings

Evaluating Performance Management

The information technology security plan should have several of the following common elements:

- Systems security activities, such as security plan and configuration documentation, implementation of minimum-security baselines, hardening of systems, maintenance of proper patch levels on systems, and investigation of new technologies
- Monitoring activities, such as network- and host-based intrusion detection implementation and management, and gathering log activity and reviewing it for violations in security policy
- Business partner access and risk management through vehicles like trust agreements, third party security assessments, and so on
- New project security design, participation, and implementation including risk assessment and the recommendations of appropriate security technology commensurate with the risk
- Security architecture design and implementation for the network, data systems, and interfaces

Evaluating Performance Management

Evaluating Business Continuity Management

- Processes for inventorying all relevant information technology and systems; determining how they interact, their relative needs for recovery capabilities, and the dependencies of these systems on each other and external factors; and for reconciling of all of these interactions along with their business requirements into a prioritized list of what steps a recovery process should follow
- Processes for identifying hot sites, cold sites, or warm sites from which to recover when warranted, and ensuring that a relationship exists with an alternative processing arrangement
- Training for both the users, to employ alternative procedures during recovery situations, and IT personnel, to perform the recovery of technologies
- Maintaining the viability of the recovery plan through testing, review, and modification processes on a periodic and documented basis

Evaluating Performance Management

Evaluating Business Continuity Management

- Communicating the realistic expectations and alternatives for business continuity along with responsibilities and tasks required during recovery scenarios to all affected parties
- Sufficiently and properly storing back up media and related processes including current recovery documentation, procedures, and stop gap processes for services that may be temporarily set aside in the throws of a recovery-in-progress, such as a security audit and management oversight processes
- Ensuring that all applicable legislative and regulatory issues are considered and appropriately addressed in the planning and execution of recovery processes
- Ensuring that processes have been considered, documented, and tested to recover the business processes, transactions, and operations to the point of the failure
- Appropriately protecting processing and information assets during recovery processing