### Methodology Assessment

<table>
<thead>
<tr>
<th>Presence of a formal process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process documentation – approved senior IT leaders</td>
</tr>
<tr>
<td>Project Plan</td>
</tr>
<tr>
<td>Mandatory sign-offs at each stage gate</td>
</tr>
<tr>
<td>Required “go / no-go” decision points</td>
</tr>
<tr>
<td>Standard templates and forms</td>
</tr>
<tr>
<td>Standard naming conventions</td>
</tr>
<tr>
<td>Escalation processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exception protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formalized testing methods</td>
</tr>
<tr>
<td>Source Control</td>
</tr>
<tr>
<td>Peer Review</td>
</tr>
<tr>
<td>Change control process</td>
</tr>
<tr>
<td>Standard project management templates / reports</td>
</tr>
<tr>
<td>Test environment separate from production</td>
</tr>
<tr>
<td>Formal reporting processes / templates</td>
</tr>
<tr>
<td>Consistent use of metrics (red, yellow, green)</td>
</tr>
</tbody>
</table>
Stakeholder involvement and engagement (legal, security, finance, audit, etc.)

Issue and Action logs

Quality Review Board / Function

Defined Documents: Requirements, Design, Testing, etc.

Centralized place for storing documents

Methodology Assessment

- Exists, is adhered to and is used by all projects
- Provides flexibility to support project sizes and types
- Provides sufficient structure to help PMs and reduce the risk of project failure
- Is based on best practices
  - PM: PMBOK, PRINCE2, etc.
  - Technical: SDLCs, SEI, etc.
  - Regulatory and Legal as required

Auditors should ensure the methodology
Types of Project Engagements

- Methodology Assessment
- Project Risk Assessment
- Readiness Assessment
- Key Phase Review
- Post-Implementation Review
- Advisory Services

Advisory Services

**Why**
Ensure proper controls, security, audit trails, etc. are included

**When**
During all key phases of the project

**How**
Being involved with project, reviewing requirements, etc.
### Why Be Involved?

The utilization and reliance upon technology to manage and support the business has increased exponentially over the last two decades. Companies continue to invest in technology to reduce admin costs, increase efficiencies and achieve competitive advantages. Proactive controls consulting will result in appropriate controls being implemented early in the development process.

IT Auditing has evolved into a necessary requirement to manage and govern an organization's risk and compliance posture.

### Corporate Executive Board

**Project Management is an audit area of concern**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Loss: late projects change cost-benefits, and could harm company's reputation.</td>
<td></td>
</tr>
<tr>
<td>Failed business expansion: implementation failures may impact income revenue stream and affect business partners / customers.</td>
<td></td>
</tr>
<tr>
<td>Inadequate IT controls: technology upgrades are expensive and can have adverse affects if not implemented properly.</td>
<td></td>
</tr>
<tr>
<td>Misaligned strategy: projects not aligned with corporate strategy may not add expected value.</td>
<td></td>
</tr>
<tr>
<td>Repeated mistakes: failure to analyze completed projects cannot rectify process inefficiencies in future projects.</td>
<td></td>
</tr>
</tbody>
</table>
### SDLC Risks

<table>
<thead>
<tr>
<th>Risk</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadequate controls in the SDLC process</td>
<td>Adoption of inappropriate SDLC for the application</td>
</tr>
<tr>
<td>Inappropriate technology and architecture</td>
<td>User requirements and objectives not met by the application</td>
</tr>
<tr>
<td>Inadequate project management</td>
<td>Inadequate stakeholder (including internal audit) involvement</td>
</tr>
<tr>
<td>Inadequate testing</td>
<td>Inadequate project management</td>
</tr>
<tr>
<td>Inadequate stakeholder (including internal audit) involvement</td>
<td>User requirements and objectives not met by the application</td>
</tr>
<tr>
<td>Inadequate stakeholder (including internal audit) involvement</td>
<td>Inadequate project management</td>
</tr>
<tr>
<td>Inadequate testing</td>
<td>Inadequate testing</td>
</tr>
<tr>
<td>Inadequate project management</td>
<td>Inadequate project management</td>
</tr>
<tr>
<td>Inadequate testing</td>
<td>Inadequate testing</td>
</tr>
</tbody>
</table>

### SDLC Risks

<table>
<thead>
<tr>
<th>Risk</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance criteria not being met</td>
<td>Inappropriate resourcing / staffing model</td>
</tr>
<tr>
<td>Inappropriate resourcing / staffing model</td>
<td>Insufficient attention to other dependencies</td>
</tr>
<tr>
<td>Insufficient attention to other dependencies</td>
<td>Inadequate configuration management</td>
</tr>
<tr>
<td>Inadequate staffing skills</td>
<td>Inadequate contractual protection</td>
</tr>
<tr>
<td>Insufficient documentation</td>
<td>Inadequate adherence to chosen SDLC</td>
</tr>
<tr>
<td>Inadequate contractual protection</td>
<td>Insufficient attention to other dependencies</td>
</tr>
<tr>
<td>Inadequate adherence to chosen SDLC</td>
<td>Inadequate configuration management</td>
</tr>
<tr>
<td>Inadequate training</td>
<td>Poor planning for data conversion and cutover</td>
</tr>
<tr>
<td>Inadequate training</td>
<td>Post cut-over disruption to business</td>
</tr>
<tr>
<td>No disaster recovery process</td>
<td>Inadequate training</td>
</tr>
</tbody>
</table>
1. User Involvement: Business and IT users are involved with key consensus-building, decision-making, and information-gathering processes.

2. Executive Support: Key executives provide alignment with business strategy, as well as financial, emotional, and conflict resolution support.

3. Clear Business Objectives: Stakeholders understand the core value of the project and how it aligns with business strategy.

4. Agile Optimization: Project uses iterative development and optimization processes to avoid unnecessary features and ensure critical features are included.

5. Emotional Maturity: Project manager directs the emotions and actions of project stakeholders and avoids ambition, arrogance, ignorance, abstinence, and fraudulence.

6. Project Management Expertise: Organization uses project managers who understand the basic skills and practices, such as certified PM Professional from the Project Management Institute.

7. Financial Management: Project manager is able to manage financial resources, account for project budget/costs, and demonstrate the value of the project.

8. Skilled Resources: Skilled project personnel are acquired, managed, retained, and controlled to move forward in the face of turnover and other personnel hurdles.

9. Formal Methodology: There is a predefined set of process-based techniques that provide a road map on when, how, and what events should occur in what order.

10. Tools and Infrastructure: The project infrastructure is built and managed with tools that enable management of tasks, resources, requirements, change, risks, vendors, user acceptance, and quality management.
Selection of Engagements

Conduct a risk analysis to identify projects or initiatives that present the greatest risk using enterprise resources:

- Project Portfolio Management (PPM)
- Company Management
- Audit Service Management Mandates
- Corporate Compliance
- Regulatory Oversight Office - Privacy
- Demand Management: Risk Assessments

Business Case

Risk Model

Engagement Selection

Audit Approach

- **Review the SDLC process**
  - Ensure proper controls are built in
  - Test on an annual basis

- **Perform Pre-Implementation Audits**
  - More time consuming
  - Value add
  - Risk based approach

We do the first one annually. I have always believed that audit sb doing more advisory work. We need to ensure that the SDLC process is followed but more value in the other. So, what are the phases and how much time?
**SDLC Phases**

- Initiation & Planning
- Requirements and Analysis
- Logical Design
- Physical Design
- Unit Testing
- System / User Acceptance Testing
- Production Prep
- Install / Post Install

**Things to Look for...**

- System Development Life Cycle (SDLC) processes
- Analysis and programming
- Data structures
- Security
- Data Controls
- Documentation
- User procedures
### SDLC Methodology

- Initiation & Planning
- Analysis
- Design
- Implementation
- Maintenance

### SDLC - Design

Controls need to be designed into the system

- Security
- Balancing
- Edits
- Quality Assurance
- Output
- Database Administration
Points in the process where authorizations are required to go on to the next step

Formal testing procedures and user sign-off

Documented procedures and User Training prior to 'Go Live'

Edits / Balancing

Security

Traceability

Standard templates and forms

Consistent use of metrics (red, yellow, green)

Escalation process

Issue and Risk logs

Change management processes

Central documentation repository
## System & User Acceptance Testing

- Review test plans for completeness
- Ensure mapping of requirements to test cases / results
- Training material testing
- If conversion, control totals and processes
- Cyclical processing: daily, weekly, monthly, quarterly, year-end, rollover (year to year)
- Manual processes developed and tested

### System & Acceptance Testing

- Parallel testing plans / results
- Security modules tested
- Test errors / retesting
- Training plans executed
- Backout protocols

- **Audit Testing Guidance**
  - If time is decreased by 10%, Project Executive must approve
System & Acceptance Testing

- **Deliverables:**
  - Sign-off for System Test
  - Sign-off for Acceptance Test
  - Updated test case artifacts

Planning the Audit

**Consideration of Purpose**
- What is driving the need for the audit?
- Is it a regular audit plan?
- The need is usually directly associated with the primary objective of the audit.

**Consideration of Risk**
- Identify risk associated with the application and its associated data, sources, infrastructure and systems.
- Assess the impact on the audit objectives, audit plan, audit scope and audit procedures.

**Functionality**
- Determine purpose of the application and verify functionality against requirements
- Verify end-user acceptance for newly installed application
- Special considerations: Security, Operational controls, Financial controls
- Verify various scenarios to understand/test functionality?
Consideration of the Control Environment

The audit plan should take into account the control environment surrounding the application, within the context of the audit purpose.

If the primary purpose of the audit is auditing proper functionality, the controls might be application development controls or systems development life cycle (SDLC) controls. In particular, controls for testing the application are important.

Consideration of Scope

- Determine relevant technologies and controls associated with auditing the applications
- Interfaces to other applications
- Source systems
- Target/destination systems
- Infrastructure or components
- Databases
- Staging area/testing facility

Determine Audit Objectives

- **Efficiency**
  - Development cost
  - Operational performance
  - On going maintenance

- **Effectiveness**
  - Meets information requirements/functionality
  - The original authorization purpose
  - Integration with other IT areas/applications
  - Operational performance

- **Compliance**
  - Laws and regulations
  - Contractual requirements
  - Customer requirements

- **Financial reporting implications**
  - Data integrity
  - End user controls

**IT General Controls**
Map Systems and Data Flows

- Relevant IT components (description)
- The business owners or business lines
- Change management policies and procedures
- The role and impact of vendors
- Business processes
- Controls
- Access and security administration

Determine Risks

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Risk</th>
<th>Risk Area</th>
<th>Objective</th>
<th>W/P Ref.</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Invalid, inaccurate or incomplete data may cause errors in reports or accounting.</td>
<td>Data integrity</td>
<td>Evaluate data integrity checks and controls between inputs and outputs.</td>
<td>CO.1.1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Unauthorized or unintended changes to middleware may cause errors in reports/accounting.</td>
<td>Change management</td>
<td>Evaluate changes to the application for appropriate approval, tests and segregation of duties (SoD).</td>
<td>CO.1.2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Unauthorized access may cause unauthorized changes to middleware or target data, causing errors in reports/accounting.</td>
<td>Security</td>
<td>Evaluate logical access controls to the application and its reports.</td>
<td>CO.1.3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Invalid, inaccurate or incomplete processing may cause errors in reports/accounting.</td>
<td>Operations</td>
<td>Evaluate processing and documentation for appropriate controls on development and support, and error identification and resolution.</td>
<td>CO.1.4</td>
<td></td>
</tr>
</tbody>
</table>
Distinguish between customized controls and those contained in vendor software

Ask management the specific nature of controls expertise used during application development process

Perform a walk-through to determine what controls are actually in the application and how they function

Determine the tests needed

---

Access security
Logical segregation of duties (SoD)
Data validation / Data integrity
Coding
Input error correction
Batch controls (where applicable)
Disaster Recovery
Typical process controls include:
- The level of automation (e.g., fully automated, IT-dependent, fully manual)
- Job scheduler dependencies (for job processing)
- Job scheduler monitoring
- Auto calculations
- Auto reconciliations
- Auto notifications

Typical output controls include:
- Reconciliations
- Reviews
- Approvals
- Error detection/error reports or lists
- Control over physical reports

Key Controls

End User Computing

Applications that are part of a significant process
- Actuarial
- External Reporting
- Health Care Management

Managed within the business and not by IT
- Excel
- Access
- APL (A Programming Language)
- VBA (Visual Basic for Applications)
EUC Control Framework

**Governance**
- Define EUCs
- Establish Policies & Procedures
- Define Ownership
- Monitor & Report

**People**
- Define Roles & Responsibilities
- Define levels of access
- Define applications in scope

**Process**
- Define Risk Ranking Metrics
- Apply risk ranking and determine control scope
- Define and apply specific controls

**Technology**
- Define technology requirements
- Determine support strategy
- Implement technology

**Management’s Role**

Management must define what constitutes an EUC and compile a list of applications used by the user group.

With full population of EUCs, management should determine which of these is impacting the organization.

Management should assess the usage of these EUCs and determine if standard procedures are followed.

Management should develop comprehensive policies and procedures.

Management should evaluate existing policies and procedures and work to establish an organization wide version.
End User Computing

The importance of the application is categorized as:

**Low**: Applications that facilitate the workflow within the business process and have no direct impact on the financial statement.

**Moderate**: Applications that typically don’t directly feed the financial statement but could impact decisions that ultimately have a financial effect.

**High**: Applications that directly create transactions which are transmitted / loaded into the general ledger or the financial statements.

Types of Errors

**Input errors**: Errors caused by data being incorrectly entered into the application.
- Data import error.
- Manual entry error

**Logic errors**: Errors caused by inaccurate calculations or coding
- Excel formulas
- VBA or ACL macros

**Interface errors**: Error caused by incorrectly importing or exporting data with other systems
- Errors in the import or export code
- Errors in the file itself
End user programmers may not follow the same IT procedural controls, introducing greater risks.

Lack of control over downloads and spreadsheets.

Results may differ from corporate results, causing management decisions to be skewed.

Storage of data.

Transmission of data outside of the company.

Use of PSDs: flash drives, CDs, etc.

Key Facts

Application Name

Owner(s)

Users

Input Sources

Number of people with access/admin rights

Usage (finance/operations)

Complexity

Risks

Application Name
Controls Required

- Segregation of Duties
- Access Controls
- Security and Integrity of Data
- Input / Output Controls
- Documentation
- Backups
- Version Control
- Change Control
- Archiving
- Training

Disaster Recovery

"Drive thy business or it will drive thee."
—*Benjamin Franklin* (1706-1790), American entrepreneur, statesman, scientist and philosopher

"It is your business when the wall next door catches fire."
—*Horatius* (65-8 BC), Roman poet
Definition from COBIT

Disaster Recovery Planning (DRP), a key component of Business Continuity Planning (BCP), refers to the technological aspect of BCP – the advance planning and preparations necessary to minimize the loss and ensure continuity of business functions in the event of a disaster.

DRP comprises consistent actions to be undertaken prior to, during and subsequent to a disaster. It is built from a comprehensive planning process, involving all of the enterprise business processes.

Strategies include alternate site, redundant data centers, reciprocal agreements, telecommunication links, disaster insurance, BIA and legal liabilities.

Protecting Your Assets

- BCP can be a long term competitive advantage
- BCP connects to the objectives of your organization
  - What are the business plans for growth, restructuring, short/long term strategies?
- A BCP plan should have the fullest possible understanding of the important processes of the business and customers and suppliers
Purpose

- Ensure the recovery from short-term, localized errors from data and equipment
- Identify processes necessary to allow the corporation to live through a more disastrous event

Questions to Ask

- What do you do if a business location is inoperable?
- What do you do if an IT location is inoperable?
Critical activities that satisfy customers’ expectations and support overall business operations

Review information on the frequency, impact and causes of downtime

Identify the critical business information needed for these activities to succeed

Identify and rank your most vulnerable business activities

Enterprise View

Enterprise Risk Management

Business Continuity Management

Disaster Recovery

Helpful Hints
Legacy systems must be adequately protected against hacker intrusion and viruses.

Place business continuity and disaster recovery on the board agenda.

Maintain a functional area checklist to continue business effectively in the case of a disruption or emergency.

Ensure change control keeps your continuity plan current with process and technology changes.

Business Continuity Plans

- Have critical business functions been identified?
- Have alternate worksites been identified?
- Are all procedures documented, reviewed and tested?
- Have call-out lists been created and updated?
- Have technical components been identified – PCs, phones, supplies, ?
- Has a “dry run” been executed recently?
Disaster Recovery Plans

- Are there short-term backup copies of data to enable recovery from a processing failure?
- Are there regular backups at scheduled intervals?
- Are there multiple generations of backups?
- Are there full system backups for the operating system and application systems?
- Are the backups stored properly?
  - Off-site
  - Vaults

Audit Focus

- Policies & Procedures
  - Updated
  - Complete
  - Approved

- Exercises
  - Frequency
  - Scope
  - Reporting

- Exercise Documentation
  - Goals & Objectives
  - Approaches
  - Assumptions
  - Participants
  - Evaluation
Audit Focus

Were the goals and objectives met?

What to do differently next time

Issue Logs reviewed and answered

Action items identified

Evaluation

What Is IAM?

Identity and Access Management (IAM) attempts to address three important questions:

Who has access to what information?

Is the access appropriate for the job being performed?

Is the access and activity monitored, logged, and reported appropriately?
Why Implement IAM?

- Improve regulatory compliance
- Reduced information security risk
- Reduce IT operating and development costs
- Improve operating efficiencies and transparency
- Improve user satisfaction
- Increase effectiveness of key business initiatives

Concepts Related to IAM Process

- Identity
  - The elements used to uniquely describe a person or machine.
- Access
  - The rights that the identity was granted.

<table>
<thead>
<tr>
<th>Provision</th>
<th>Administer</th>
<th>Enforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>Monitor</td>
<td>Authenticate</td>
</tr>
<tr>
<td>Validate</td>
<td>Manage passwords</td>
<td>Authorize</td>
</tr>
<tr>
<td>Approve</td>
<td>Audit and reconcile</td>
<td>Log activity</td>
</tr>
<tr>
<td>Propagate</td>
<td>Administer policies</td>
<td></td>
</tr>
<tr>
<td>Communicate</td>
<td>Strategize</td>
<td></td>
</tr>
</tbody>
</table>

Information Systems and Data

Components
- Processes
- Activities
**Concepts Related to IAM Process**

**Provisioning**
- Refers to an identity’s creation, change, termination, validation, approval, propagation, and communication.

**Administration**
- Includes establishment of IAM strategy, monitor the provisioning process, manage passwords, etc.

**Enforcement**
- Includes authentication, authorization, and logging of identities as they are used within the organization’s IT systems.

---

**Diagram of a Provisioning Process**

1. Any person or system submits a request.
2. Manager or security administrator approves the request.
3. Application owner approves the request.
4. Target application automatically grants access.

- Segregation of duties roles
- Approval workflow
- Entitlement repository
- Entitlement configuration roles
Identify certain key elements when assessing a company’s IAM posture.

- Aligning business and management units
- Understanding existing laws and regulations
- Establishing budgets
- Developing achievable implementation plans
- Defining how technology can enable a more effective control environment
Auditing IAM

- Assess the organization’s IAM strategy, provisioning process, and enforcement process.
- Document identities, identity repositories, and identity lifecycle components.
- Determine controls within identity lifecycle process.
- Document access right, its repositories.
- Determine controls related access rights.
- Test the process especially terminations.

Testing IAM

**New Users / Modifications**
- Get a system-generated list (population) of change requests.
- Select a sample (usually 20-50 changes or 10-20%, whichever is smaller).
- Request change forms and review them for evidence of key controls.

**Removals**
- Get a list (population) of terminated employees.
- Select a sample (usually 20-50 changes or 10-20%, whichever is smaller).
- Observe system and determine if the user accounts are disabled or removed.
- Ensure timeliness meets company standards.
User Recertification

Regularly re-validate all users’ access levels on all systems

- Excessive levels of access
- Terminated users
- Potential process problems

Detective control throughout the year

- Ensure it is done
- Ensure the population is complete

Access Management

Does everyone have access to what they need for their jobs and can unmanaged devices attach to our network?

- Principle of least privilege
- Centralized user directory
- Access reviews
- Password management
- Lock screens
- Multi-factor authentication
- Port security

How do we secure new systems before adding to the network, is there production data in non-production systems?

- System hardening process
- Software Development Lifecycle (SDLC)
- Change control procedures and Change Approval Board (CAB)
- Vulnerability management procedures
- Development, QA, Production
- Scan EVERYTHING (hosts, databases, apps)
- Penetration testing (validate your controls)
IAM Risks

**Provisioning**
- Lack of evidence supporting system level access with authorizations
- Lack of guidance when provisioning user access leading to SOD issues

**Periodic Review**
- Complex and decentralized environments create challenges to properly review access
- Managers just "signing off" without a detailed review
- Processes are inconsistent and not properly documented

**Removal**
- Reliability on manual controls
- Insufficient monitoring procedures to compensate for reliance on manual controls