

INFORMATION  
MANAGEMENT  
& TECHNOLOGY

**Information Technology Risks & Controls  
for Financial Systems**

PEM-PAL Treasury CoP Workshop 2011

Kristin Lado Tufan



# Introduction

- IT Risk and Compliance Officer in Information Management and Technology (IMT) of the World Bank; CISA, CRISC Certifications
- Managed the Bank's Internal Controls over Financial Reporting (ICFR) IT General Controls from 2007 to date
- In 2000 – 2005 timeframe, advised Development Gateway Grantees in Mongolia, Sri Lanka, and Eastern Caribbean (with Romania) on web-based business plans and implementation to support Ministries and Donors
- The World Bank voluntarily complies with ICFR (similar to US Sarbanes-Oxley) as a good practice
- The Bank's in-scope applications include SAP, PeopleSoft, and numerous Treasury applications
- Complying with ICFR is not just a one-time event, it's a way of doing business

# Agenda

- ▶ Overall internal control environment to provide reasonable assurance of the completeness, accuracy, and integrity of your FMIS for financial reporting
- ▶ Frameworks to assist in implementing processes and controls
- ▶ Specific Operational and Information Security Controls for each layer of your FMIS
- ▶ World Bank Example of a Secure Web Portal



- “Trust is not a control”
- “Do what you document, and document what you do”

# The Bank's Context...

- ▶ **SAP:** Global ERP with 24,000 users; 12+ major applications, including standard modules such as AP/AR and in-house developed applications for loan disbursement and travel; approximately 8.6 million transactions per month
- ▶ **PeopleSoft:** Global ERP with approximately 18,500 dynamic roles/users and 1,033 static roles; total of 3,756 transactions assigned; Supports Human Resources, Payroll, Pensions processes
- ▶ The Bank has an in-house developed **secure website (Client Connection)** that offers government officials and project implementing agencies quicker access to information about their portfolio and the Bank's country analytic work
- ▶ The Bank also has numerous **Treasury applications** to support Treasury Operations
- ▶ **Remote Access:** The Bank has several options for Remote Access, all enabled with two-factor authentication
- ▶ Currently, a total of **148 key controls** are tested each year across all financial systems in scope for Internal Controls over Financial Reporting (ICFR)

# Some Information Technology Risks To Financial Systems

- ▶ **Unauthorized Access:** User/Developer access was not approved for a particular level of access or action; Example: Ensure privileged access is appropriately restricted.
- ▶ **Excessive Access:** User/Developer access level is beyond the scope of job role and responsibility; Example: Ensure the Principle of Least Privilege is in place – people only have access to the information and transactions needed to perform their job and scope of responsibility
- ▶ **Unauthorized Changes:** Program change was not approved before move to production; Example:
- ▶ **Fraud** is a potential result of these risks if actions are intentional
- ▶ **Lack of control** around the acquisition and implementation of new applications and maintenance of existing applications
- ▶ **Lack of control** around the acquisition, installation, configuration, integration, and maintenance of the IT infrastructure.

# Internal Control Environment

## ▶ Entity-level Controls

- ▶ Tone at the Top and culture of the organization
- ▶ Management ensures that the policies and procedures are in place and all employees are aware and adhering to them

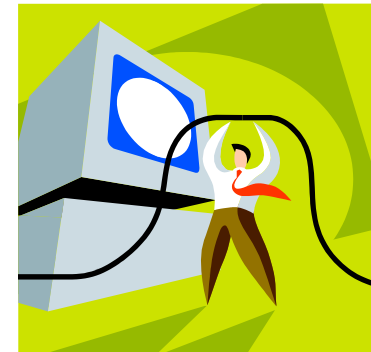
## ▶ Application Controls

- ▶ Application Development and Maintenance
- ▶ Access to Programs and Data/Information

Security Controls (applies to all layers)

## ▶ Information Technology General Controls

- ▶ Infrastructure Change Management: Database, System Software, Network
- ▶ Information Systems Operations: Batch Job Processing, Backup and Restore



## People, Process, Technology

# Useful Frameworks as a Foundation for the Internal Control Environment

- ▶ **COSO/COSO ERM** (The Committee of Sponsoring Organizations of the Treadway Commission): Integrated framework for internal controls, focuses on the Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring
- ▶ **COBIT** (ISACA): Control Objectives for Information Technology that focuses on four key domain areas of Plan & Organize, Acquire & Implement, Deliver & Support, and Monitor & Evaluate
- ▶ **ITIL** (Information Technology Infrastructure Library) Framework for IT Service Management practices, such as Change Management, Incident Management, Problem Management, Configuration Management, Service Level Management
- ▶ **CMMi** (Software Engineering Institute): Capability Maturity Model Integration for Software Development Lifecycle
- ▶ **ISO20000**: Framework and Certification for IT Service Management
- ▶ **ISO27001**: Framework and Certification for Information Security
- ▶ **RiskIT** (ISACA): IT-related business risk, focusing in Risk Evaluation, Risk Governance, and Risk Monitoring/Reporting

# Application Development and Maintenance

- ▶ **Key Risks:** Unauthorized Access/Changes, Excessive Access, Fraud; Ineffective Controls in Process
- ▶ **Document** process and identify key controls; support with a workflow tool
- ▶ **Segregation of Duties** (for business and IT)
  - ▶ Separation between the development and production environments;, for example, Developers should not have update access to the production environment
  - ▶ All changes to the production application should be documented and approved; the person who initiates change should be different from the one who approves the change, and different from the person who moves the change to production
- ▶ **Access**
  - ▶ User Access: Based on Job Roles and Responsibilities
  - ▶ Privileged Access: Clear authorization, strong authentication;
  - ▶ Rule of Least Privilege – the access needed to perform one’s job



# Infrastructure Change Management

- ▶ **Key Risks:** Unauthorized Access/Changes, Excessive Access, Fraud
- ▶ **Document** Change Management Policy, Processes and Controls; support with a workflow tool
- ▶ Use a risk-based approach for changes: Emergency to Major Changes; varying levels of documentation and approvals required
- ▶ **Segregation of Duties:** the person initiating the change should be different from the one approving the change, and different from the one moving the change to production
- ▶ Ensure roles and responsibilities are clear regarding who can initiate a change, test the change, approve, and move to production
- ▶ Ensure all evidence of changes are documented, approved, and stored for easy retrieval



# Information Security Controls: Access

- ▶ **Authentication and Authorization:** How access is achieved and who approved – new user and transfer
- ▶ **Privileged Access:** System Administrators
  - ▶ Ensure terminated employees access rights are removed timely
  - ▶ Individual vs. Service Accounts – traceability
- ▶ **Data Security and Integrity** – Secure data transfer; encrypt data in transit (Secure Socket Layer/SSL and Secured Hypertext Transmission Protocol/HTTPS)



- ▶ **Network and Web Application Firewalls:** Review Logs, restrict access
- ▶ **Passwords for all user types:** Complex, force change, account lockout
- ▶ **Physical Security** at your Data Center – who has access to what; is it approved and reviewed periodically?

# Information Systems Operations/ Contingency Planning

- ▶ **Key risks:** System failure, Data Loss; Ineffective Controls in Process
- ▶ **(At a minimum) Document Backup and Restore Processes**
  - ▶ Monitor failures and take action
  - ▶ Perform periodic restore tests to ensure data availability from tape/disk
  - ▶ Secure, off-site storage
- ▶ Develop an IT Disaster Recovery Policy; Test the IT Contingency Plan
- ▶ Document Batch Job Processes
  - ▶ Who has access to run?
  - ▶ Know the scope, impact and frequency of jobs
  - ▶ Take action on failed jobs

# World Bank Example: Client Connection

- ▶ Client Connection is a secure web-based portal that allows Borrowers/Recipients and Donors access to information related to loans, credits, grants, and trust funds
- ▶ Straight Through Processing (STP) is the newest phase of the eDisbursement project – Bank clients can submit an online disbursement request and sign electronically
- ▶ Authorized Signatories and Beneficiaries must be approved and pre-registered
- ▶ Separate Profiles, such as a Form Creator and a Form Signatory, must be in place
- ▶ Different profiles have different levels of access or different types of transactions they can perform
- ▶ Access is granted with a valid user id and passcode, which includes a pin and dynamic token

# http://clientconnection.worldbank.org

The screenshot shows the homepage of the World Bank Client Connection website. At the top left is the World Bank logo and the text "World Bank". To the right of the logo is the text "Request Registration Information | Feedback". Below this is the "Client Connection" logo. The main content area features a large image of a woman in traditional red headgear and glasses, smiling. To the right of the image is a "Welcome to World Bank's Client Connection" message, explaining that users can access project and financial information, process procurement documents, and access knowledge resources. Below the image is a banner for "Millennium Development Goal 3: Promote gender equality and empower women". To the right of the main content is a "Registered User" section with a "Login" button and a "Forgot/Reset Password" link. Below the main content is a "Secure Site" link. The page is divided into two columns: "News / Announcements" and "Related Links". The "News / Announcements" column contains a link to "Financial Management" with a brief description and a "Full Story" link. The "Related Links" column contains five links: "World Bank Home", "Development Gateway", "Financing and Risk Management", "About the Trust Fund Donor Center", and "World Bank Finances". At the bottom left is a "Feedback | Request Registration Information" link.

**World Bank** Request Registration Information | **Feedback**

## Client Connection

**Welcome to World Bank's Client Connection**

From this site you can access your country's project and financial information; process procurement documents over the internet and access the World Bank's knowledge resources.

Log in to take a site tour and learn more about the site's functionality.

**Registered User**  
**Login**  
[Forgot/Reset Password](#)

**Secure Site**

**Millennium Development Goal 3**  
**Promote gender equality and empower women**

### News / Announcements

[Financial Management](#)

Financial management, procurement and disbursement arrangements are core elements of the fiduciary framework for World Bank's operations.... [Full Story](#)

[Welcome to Client Connection!](#)

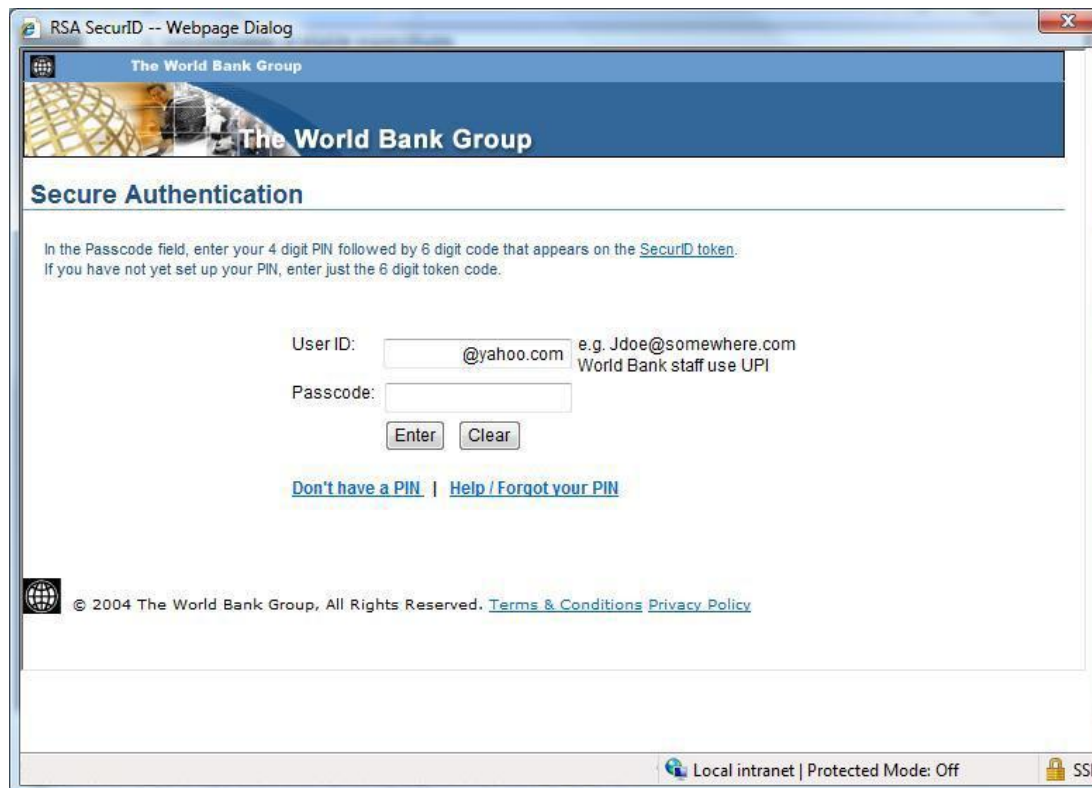
### Related Links

- [World Bank Home](#)
- [Development Gateway](#)
- [Financing and Risk Management](#)
- [About the Trust Fund Donor Center](#)
- [World Bank Finances](#)

[Feedback](#) | [Request Registration Information](#)

# Using Two-Factor Authentication...

- User id
- 8 digit PIN
- Dynamic 6 digit token code



The screenshot shows a web browser window titled "RSA SecurID -- Webpage Dialog". The page header features "The World Bank Group" logo and name. Below the header, the section is titled "Secure Authentication".


In the Passcode field, enter your 4 digit PIN followed by 6 digit code that appears on the [SecurID token](#).  
If you have not yet set up your PIN, enter just the 6 digit token code.

User ID:  @yahoo.com e.g. Jdoe@somewhere.com  
World Bank staff use UPI

Passcode:

[Don't have a PIN](#) | [Help / Forgot your PIN](#)

© 2004 The World Bank Group, All Rights Reserved. [Terms & Conditions](#) [Privacy Policy](#)

Local intranet | Protected Mode: Off 

# eForm Example

STP is enabled, Signature is Pending...

**Loan Overview** | **Disbursements** | **Repayments** | **eForms**

e2380 | eSignatories | Beneficiary Registration

Straight Through Processing has been enabled for this loan. [eForm Help](#)

**Create new e2380 - Application for Withdrawal**

Application type: Select

Beneficiary: Select

Delete Application Application Locked by Another User Show Transaction Detail Archived Documents

**Existing applications**

Application type: All

| Borrower reference        | Status               | Last Updated | Date Sent to the Bank | Application type |
|---------------------------|----------------------|--------------|-----------------------|------------------|
| <a href="#">TST IK 05</a> | Pending Signature(s) | 09-Nov-2010  |                       | Direct payment   |

# Signing the Form...

## B. Payment instructions

|   |  |   |  |
|---|--|---|--|
| 6a. Application currency<br>United States Dollars   | 6b. Application amount<br>5,750,125.79 | 6c. Equivalent payment currency (if different from application currency)  |  |
| 6d. Application amount (in words)<br>United States Dollars FIVE MILLION SEVEN HUNDRED FIFTY THOUSAND ONE HUNDRED TWENTY-FIVE AND 79 |  |   |  |
| 7. If the application covers more than one loan (as specified in item 2 above), please provide amounts allocated to each financier. |  |   |  |
| Loan/Financing/Grant No.(s)   | Amount                                 | Loan/Financing/Grant No.(s)   | Amount   |
|   |  |   |  |
| Loan/Financing/Grant No.(s)   | Amount                                 | Loan/Financing/Grant No.(s)   | Amount   |
|   |  |   |  |
| 8. Name and address of beneficiary<br>NATL HIVAIDS CONTROL PROJ III<br>1234 ANYWHERE IN NEW DELHI                                   |  | 9. Amount to be paid in installments?<br>No<br>(if yes, complete "Requested Schedule for Advance Payments" Form 2381) |  |
| 10a. Name and address of the beneficiary's bank<br>BANK OF BARODA<br>MADHUBAN: NEW DELHI  |  | 10b. Account number (or IBAN for euro payments) of the beneficiary at the beneficiary's bank<br>CHARITO ACC 123       | 10c. SWIFT code of the beneficiary's bank<br>BARBINBBNND |
| 11a. Name and address of the intermediary bank<br>FEDERAL RESERVE BANK OF NEW YORK<br>FLOOR 7: NEW YORK                             |  | 11b. Account number (or IBAN for euro payments) of the beneficiary's bank at the intermediary bank                    | 11c. SWIFT code of the intermediary bank<br>FRNYUS33XXX  |
| 12. Special payment instructions(if any)  |  |   |  |



The supporting documentation contains 1 electronic document(s).

1 more signature(s) still needed(to access the eSignatories tab, click [here](#))

I have read the certification appearing on this form and agree to its terms.

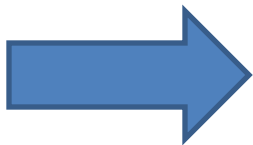
Sign

Reject

Cancel

### Supporting Documents

| Documentation Type/Name   | Size | Attached By                                     |
|---|------|---|
| Statement of Expenditure<br><a href="#">STP Statement of Expenditures.xls</a> | 16KB | STP Create User3<br>26-OCT-2010<br>06:02 PM EST |





# Methods for Preventive and Detective Controls

- ▶ Segregation of Duties: Operational and Privileged Access
- ▶ Two-Factor or Multi-factor Authentication
- ▶ Periodic Review of Roles and Access at all layers, from network access to application access
  - ▶ Perform at least every six months; document review and action taken
- ▶ Continuous Controls Monitoring – automated and manual
  - ▶ Monitor access to systems - Repeat failed logon requests and unauthorized access
  - ▶ Monitor changes from the source (application/database/operating system) and compare with changes logged in ticketing systems
  - ▶ Monitor firewall activity
- ▶ Encrypt Data in Transit
- ▶ Consider an Application Firewall



# Benefits of an Audit

- ▶ Audits can provide reasonable assurance that the financial statement preparation is supported by adequate and sustained internal control compliance
- ▶ Audits may uncover deficiencies in information system processing that when remediated, will strengthen the control environment and the integrity of the system
- ▶ View an audit as an opportunity for process and control improvement, control rationalization, and assurance that the operation is running efficiently and effectively

- ▶ View Auditors as



Strategic Partners!

# Questions and Comments?

