ME

(203) 726-1711
TN-VISA (2015-08-27)
I-140, H1-B (2017-10-17 to 2020-09-06)

Elevator

♦I am an {seasoned/accomplished/expert} information security compliance project manager. I specialize in this field because I have seen compliance become a business enabler ♦I enjoy being at the forefront of my organization' security endeavor. I am proud being the 3rd line of defence because I have seen compliance become a business enabler (HOOPP, CBOC) ♦I have accumulated throughou the years a vast wealth of experiences, professional qualifications and competencies so that I can navigate through complex systems, ambiguity; so that I can manage multiple project assignments; and so that I can interact with subject matter experts to understand how key code elements address specific risk (ITD test) ♦I like leading and championing for positive change ♦I am ready to apply my risk and compliance expertise in of internal controls to help grow <your company> ♦As a management consultant, I learned fast and can be effective on day one (PWU Consultant). I consciously seek to comprehend people, process, technology, goals. I stay alert thru self-challenges and by stepping out of own comfort zone and by being thoughtful, well-researched actions ♦I have experience working with acquisitive companies ♦I enjoy working in a dynamic environment ♦I delivered complex business solutions through partnership with stakeholders from multiple disciplines – from front office to risk, treasury, accounting, operations and technology ♦I have over 20 years of experiences in financial services, capital markets, retail and insurance. I held managerial roles at SCOTIA, CIBC, Sierra, AIG (Hong Kong), Price Waterhouse (Australia) and most recently a delivery manager at SCOTIA, HOOPP, project manager/ controller CIBC and Sierra, PMO head at AIG (Hong Kong) and manager at PW (Australia) ♦I am passionate about technology and am able to focus on key issues and the details that come with it ♦Ability to interact confidently with all levels, to set objectives, and to drive results ♦I can provide consultative support to business partners to identify opportunities for control improvements with the objective of mitigating risk and improving compliance and operational performance. In this capacity ♦I specialize in the realization of organizational strategies by implementing best practices in project and finance management to deliver portfolios, programs and projects. ♦I developed a reputation as somebody who creates value by bridging business and technology considerations into a holistic view of the process at hand. ♦Experience in: technology consulting, system auditing, privacy, cyber-security, e-commerce, e-money licensing, digital or online advertising, cloud, online payment regulations, anti-money laundering, online media and entertainment, online content licensing royalty management, software development, supply chain systems and processes, hardware manufacturing, financial processes and systems, mergers and acquisitions, large project systems integration, risk management, or data analytics Experience with internet technology from a technical, regulatory, or commercial perspective ♦Hands-on with technology, budgeting, planning, system design, testing

Personal Effectiveness Equation

Attitude-Ability + Alliances-Assignments

Strengths

ABILITY ❶Learn from experience ❷Big picture ❸Recognize expertise ATTITUDE ❶Collaborative ❷Intellectual curiosity ❸Promote healthy context ASSIGNMENT ❶Beyond comfort zone ❷Hands-On ❸Value/Impact ALLIANCE ❶Teamwork ❷Recognition ❸Communicative

Weaknesses

❶**Quantitative** but numbers do not capture the totality of human experience and the essence of what it is to be human ❷**Details-oriented** insist in examining every angle of Rubik's cube -> can be distracted. Now start a day with clear objectives, agenda. Think in perspectives, future ❸**Perfectionist** Expected top performance. Now take into account people perspectives. Develop empathy to better motivate. Develop plan to account for deviations. Slow/Fast thinker. Appoint right person for job instead of best all-rounder

Further questions to ask interviewer

Is this a new position? How long has this position existed? What significant changes do you foresee in the near future? How is your organization structured? How many portfolios? How many professionals? How is information shared? How is performance measured? What are my main responsibilities? Who will I report to? Who will report to me? How do I fit in the department? What is the organization's main goal? What are the organization's long term plans? What provisions are there for skills acquisition? What career progressions within the organization does this job entail? How does this organization differ from its competitors? What does a typical day in the post entail? What additional information can I provide about my qualifications? What are the next steps in the selection process?

Closing

Would you like a list of references? - What are the next steps? - When can I expect to hear from you? - Are there any other questions I can answer for you? Thank you again for having me here today. From the information that you have been sharing with me, I am even more excited over this opportunity at … As you can see, my experience has been with finance, and my skills risk management, financial instruments, business analysis, quantitative modeling and IT architecture.

Tech Talk

AWS Technology

AWS Python SDK BOTO3 supports AWS cloud services, including Elastic Compute Cloud, DynamoDB, AWS Config, CloudWatch and Simple Storage Service SERVICES •Elastic Compute Cloud (EC2), a service for provisioning computing resources on demand •Elastic Load Balancing (ELB) distributes traffic to a bunch of servers behind it. Highly available by default.•Simple Storage Service (S3), online storage for opaque data •Elastic Block Store (EBS), persistent disk-like storage for EC2 instances, in 2008 •Elastic MapReduce (EMR), a service providing Hadoop-like clusters for running MapReduce (and later Apache Hive and Apache Pig) jobs, in 2009 •Relational Database Service (RDS), a service for managing relational database server instances running in AWS, also in 2009 ELEMENTS ♦Instance types: heavy compute capability, vast storage, economy, or simply general-purpose use ♦Availability zones independent within a region, but faster interconnections ♦Temporary instance can disappear after some time ♦Images what instances are running: operating system type and version, the software packages that are available, and applications that are installed. These considerations are all bundled up into images ♦CIDR (Classless Inter-Domain Routing) IAM ♦Config Asset Mgt [(Network Asset Mgt [Database Asset Mgt (Data)])] ♦IAM policy ♦AWS root account SECURITY ♦Security groups AWS service to control network traffic like a firewall. Security groups can be attached to services like ELB, EC2, and RDS. With security groups, configure load balancer so that it only accepts requests on port 80 from the internet, web servers only accept connections on port 80 from the load balancer, and MySQL only accepts connections on port 3306 from the web servers. If you want to log in to your web servers via SSH, you must also open port 22. ♦Control Traffic: Allow ICMP[1], SSH ♦VPC (Virtual Private Cloud) ♦IGA (Internet gateway) ♦NAT (Network Address Translation) gateway RESOURCE PROVISIONING ♦CloudFormation – Elastic Beanstalk – OpsWorks ♦CloudFormation Elements: Template = JSON/YAML formatted file used as blueprint to build AWS resources; declaration of AWS resources that make up a stack Stack = collection of resources to build; Create, update and delete a collection of resources by creating, updating and deleting stacks. Changeset = user proposed set of changes to the running resources in Cloudformation stacks. Users get to see how the change set will impact running resources before implementing it ♦Cloud Template 9 components: ❶Version ❷Description ❸Metadata ❹Parameters ❺Mappings ❻Conditions ❼Transform ❽RESOURCES ❾Outputs

AWS Audit

❶GOVERNANCE ♦Understand Structure, Roles, Responsibilities ♦Establish AWS Directives ♦Define/ Understand Network Boundaries ♦Establish Complete/ Accurate Inventory ♦Classify IT Inventory ♦Accountability for IT Asset Acquisitions ♦"Manage External Providers" ♦"Protect AWS Root Accounts" ❷NETWORK CONFIG & MGT ♦Maintain Security Architecture & Network Traffic Baselines ♦Environment Segregation ♦Restrict Administrative Access ♦Maintain Valid VPC Peering Connections ♦"Network Redundancy Between Enterprise and AWS" ♦"Securely Integrate Enterprise Systems to AWS" ♦Considerations: SIEM (security information & event management) automated/manual? TOOLS (a) AWS root account, b) AWS Management Console, c) AWS Command Line Interface (CLI), d) AWS Software Development Kits (SDKs), e) PowerShell) ❸ASSET CONFIG & MGT ♦"Utilize Baselined AWS Resources" ♦Change Management ♦"Identify/ Remediate Asset Vulnerabilities" ♦"External Penetration Testing" ♦"Identify/ Remove Unnecessary Assets" ♦"Define Data Retention Requirements" ❹LOGICAL ACCESS CONTROLS ♦Secure Root Account Access ♦Establish Role-based Access ♦Segregate Duties ♦Restrict Administrative Toolsets ♦Remove Access ♦Assess Access Roles & Permissions ♦Delegate Access to External AWS Accounts ♦"Control Access to Cryptographic Keys" ♦"Enforce Session Timeouts" ♦System Use Notifications ❺DATA ENCRYPTION CONTROLS ♦Define Encryption Requirements ♦Encrypt Data by Classification ♦Secure Remote Connectivity ♦"Detect Misconfigured Encryption" ♦Considerations: S3-Bucket, RedShift-cluster, DynamoDB-table ➔ Min. AES 256-bit level encryption ❻SECURITY INCIDENT RESPONSE ♦Maintain Plan ♦Practice Plan ♦Crisis Communications ♦"Enterprisewide Visibility Through Automation" ♦"Centralized & Secured Storage of Security Events" ♦"Communicate with External Enterprises" ♦"Create Roles to Manage AWS Incidents" ❼SECURITY LOGGING & MONITORING ♦"Define Monitoring Requirements by AWS Application" ♦Configured Logging Requirements ♦Log Storage ♦Restrict Log Access ♦Monitor Log Status ♦"Set Log Retention" ♦"Review Logs for Events of Interest" ♦"Manage Logging Failure" ♦Accurate Log Timestamps ♦"Assess Adequate Logging Coverage" ♦"Detect Attempted Privilege Abuse" ❽DISASTER RECOVERY ♦"Disaster Recovery Plans: Stakeholder Input & Review" ♦Business Continuity Plans (BCPs) ♦High Availability ♦Alternating Responsible Personnel ♦Validate Backups ♦Manage Vendor Lock-in Risk

SAP Deployment

♦HANA Enterprise Cloud (HEC) ♦HANA One (database as a service) DEPLOYMENT ❶On-premises (as appliance) ❷In the cloud: AWS/ Azure/ Google Cloud Platform/ IBM Softlayer/

[1] The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached. The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes

Huawei FusionSphere/ HP Helion/ SAP HANA Enterprise Cloud (Perbyte farm, private managed cloud)/ SAP Cloud Platform (HANA Cloud Platform, PaaS) ❸"Tailored Data Center Integration (TDI)" (re-use H/W components: storage, network) LICENSING ◆Runtime License (to run SAP applications: SAP Business Warehouse powered by SAP HANA and SAP S/4HANA) ◆Full Use License (to run both SAP and non-SAP applications; used to create custom applications – Editions: Base Edition: Core database features and development tools but no support SAP applications - Platform Edition: Base edition plus spatial, predictive, R server integration, search, text, analytics, graph engines and additional packaged business libraries - Enterprise Edition: Platform edition plus additional bundled components for some of the data loading capabilities and the rule framework - Express edition; streamlined version on laptops, free of charge.

SAP Server Components

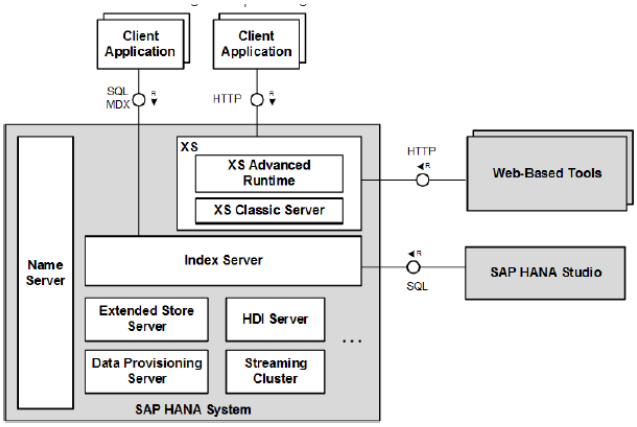


Figure 2: Main Components of the SAP HANA System

Server Component	OS Process	Service Name	Description
Index server	hdbindexserver	indexserver	The index server contains the actual data stores and the engines for processing data.
Name server	hdbnameserver	nameserver	The name server owns the information about the topology of the SAP HANA system. In a distributed system with instances of the SAP HANA database on multiple hosts, the name server knows where components are running and which data is located on which server.
XS advanced runtime	hdbxscontroller hdbxsexeagent hdixsuaaserver	xscontroller xsexeagent hdixsuaaserver	As of SAP HANA 1.0 SPS 11, SAP HANA includes an additional run-time environment for application development: SAP HANA extended application services (XS), advanced model. SAP HANA XS advanced model represents an evolution of the application server architecture within SAP HANA by building upon the strengths (and expanding the scope) of SAP HANA extended application services (XS), classic model. The SAP HANA XS advanced runtime consists of several processes for platform services and for executing applications.
SAP HANA Deployment Infrastructure (HDI) server	hdbdiserver	diserver	HDI handles the deployment of design-time artifacts into SAP HANA.
XS classic server	hdbxsengine	xsengine	SAP HANA Extended Application Services (SAP HANA XS) is the application server for native SAP HANA-based web applications. It is installed with the SAP HANA system and allows developers to write and run SAP HANA-based applications without the need to run an additional application server. SAP HANA XS is also used to run web-based tools that come with SAP HANA, for instance for administration, lifecycle management and development. SAP HANA XS classic is the original implementation of SAP HANA XS. This server can run as a separate server process or embedded within index server.
Extended store server	hdbesserver	esserver	The extended store server is part of the SAP HANA dynamic tiering option for SAP HANA. It provides a high-performance disk-based column store for very big data up to the petabyte range.
Data provisioning server	hdbdpserver	dpserver	The data provisioning server is part of the SAP HANA smart data integration option for SAP HANA. It provides capabilities such as data provisioning in real time and batch mode, real-time data transformations, data quality functions, adapters for various types of remote sources, and an adapter SDK for developing additional adapters.
Streaming cluster	hdbstreamingserver	streamingserver	The streaming cluster is part of the SAP HANA smart data streaming option for SAP HANA. Smart data streaming extends SAP HANA with capabilities of SAP Event Stream Processor for consuming data streams and complex event processing.
Accelerator for SAP ASE	hdbetsserver	etsserver	The SAP ASE server is part of the SAP HANA Accelerator for SAP ASE option for SAP HANA. It provides SAP Adaptive Server Enterprise (ASE) users the ability to use SAP HANA on SAP ASE data, for real-time analytics,
SAP HANA remote data sync	hdbrdsyncserver	rdsyncserver	The remote data sync server is part of the SAP HANA Real-Time Replication option for SAP HANA. SAP HANA remote data sync is a session-based synchronization technology designed to synchronize SAP SQL Anywhere remote databases with a consolidated database

SAP Security

◆**Cloud Security**: identity, encryption, key management, authorization, assessment, logging, and monitoring) ◆**Contract Considerations**: Event Log, Testing & Assessment, Breach Response, Certifications, SOD, Data Privacy ◆Network & Application Segmentation ◆Immutable Servers ◆Blast Radius ◆Network Visibility (rely on application security) Cloud Security Operations ◆Patching and Change Management ◆Incident Response Security Services Integration ◆**HANA Cloud Platform (HCP)** ◆Identity Management (ABAP Standard Roles, SAP NetWeaver Portal Role, Application Roles) ◆Federation and Token-based Authentication ◆Encryption ◆Key Store ◆Management Plane Application Security ◆Assessment-Monitoring-Logging and Auditing-Penetration Testing

Inbound

PROTOCOL	TCP Port	CLIENTS
SQLDBC (ODBC/JDBC)	3xx15 3xx17 3xx13 5xx14 1128 1129	Application servers SAP HANA Studio End users Replication systems
HTTP(S)	80xx 43xx	Web browsers Mobile devices SAP HANA Direct Extractor Connection (DXC)
Internal / Proprietary	3xx09	SAP Support

Outbound

SOURCE	DESTINATION
SAP Solution Manager Diagnostics Agent (SMD)	SAP Solution Manager
SAP HANA Lifecycle Manager	SAP Service Marketplace
SAP HANA XS	External Servers
SAP Smart Data Access	External data sources
SAP HANA	R environments

SAP NetWeaver

SAP NetWeaver components: ◆SAP Business Information Warehouse (data warehouse, business intelligence) ◆SAP Business Intelligence (analytics, reporting tools) ◆SAP Enterprise Portal ◆SAP Exchange Infrastructure ◆SAP Knowledge Warehouse ◆SAP Master Data Management ◆SAP NetWeaver Process Integration

SAP NetWeaver Security

❶**Authentication & Single sign-on** ◆SAP Single Sign-On ◆SAP Cloud Platform Identity Authentication ❷**Authorization and Role Management** ◆User & Role Administration of Application Server ABAP ◆User Management of the Application Server Java ❸**Secure Communication** ◆Network Security (SAP SW Ports) ◆Transport Layer Security (SSL) ◆ Unified Connectivity (UCON) for secured Remote Function Calls (RFCs) ◆ Digital Signatures and Encryption ◆Web Services Security (Security Assertion Markup Language SAML, WS-Security) ❹**Secure Operations** ◆System Security ◆Logging & Monitoring – AS ABAP (Audit Log, Audit Information System (AIS), Read Access Logging (RAL)) ◆ Logging and Monitoring – AS Java (Audit Log, Tracing & Logging) ◆Virus Scan ◆ Secure Storage (ABAP) ❺**Secure Development** ◆ABAP ◆JAVA (password, encryption) ◆User Interface: Cross-Site Scripting (XSS)/ SQL Injection/ Input Validation/ Canonicalization/ Directory Traversal/ URL Encoding and Manipulation/ Cookie Manipulation/ Clickjacking

SAP Risks

Financial Risks ◆Financial Reporting ◆Accounting Guidelines ◆Financial Market Regulations ◆Financial Misstatements ◆Internal Compliance ◆Treasury ◆Currency ◆Liquidity ◆Cost of Financing ◆Investment / Debt ◆Derivative Instruments ◆Cash Management ◆Controlling ◆Budgeting ◆Financial Planning and Forecasting ◆Cost Center Reporting Organization & Governance ◆Corporate Governance ◆Organizational Structure ◆Processes ◆Process Execution ◆Internal Controls System Operational Risks ◆Intellectual Property Rights Procurement ◆Vendor Selection Other ◆Vendor Monitoring Other ◆Vendor Dependency Other ◆Policy Other Infrastructure Operations ◆Security Governance Other Facilities and Physical Security ◆Planning and Construction Other ◆Loss of Infrastructure Other ◆Unauthorized Access Other ◆Impairment of Personnel Other ◆Facilities and Physical Security Other Information & IT ◆Confidentiality Other ◆Availability Other ◆Technology Other ◆Integrity Other ◆Information & IT Other

Network Ports

Protocol	TCP/ UDP	Port No	Description
File Transfer Protocol (FTP) (RFC 959)	TCP	20/21	FTP server can easily be set up. Provides the ability to easily relocate files from one system to another. FTP control is handled on TCP port 21 and its data transfer can use TCP port 20 as well as dynamic ports depending on the specific configuration.

Secure Shell (SSH) (RFC 4250-4256)	TCP	22	Primary method to manage network devices securely at the command level. Used as a secure alternative to Telnet which does not support secure connections.
Telnet (RFC 854)	TCP	23	Primary method to manage network devices at command level. Unlike SSH, Telnet simply provides basic unsecured connection. Many lower level network devices support Telnet and not SSH. Caution when connecting to a device using Telnet over a public network as the login credentials will be transmitted in the clear.
Simple Mail Transfer Protocol (SMTP)	TCP	25	Two functions: to transfer mail (email) from source to destination between mail servers and used by end users to send email to a mail system.
Domain Name System (DNS) (RFC 1034-1035)	TCP/ UDP	53	Used on public internet and private networks to translate domain names into IP addresses, for network routing. Hieratical with main root servers that contain databases that list the managers of high level Top Level Domains (TLD) (eg .com). These different TLD managers then contain information for the second level domains that are typically used by individual users (for example, cisco.com). A DNS server can also be set up within a private network to private naming services between the hosts of the internal network without being part of the global system.
Dynamic Host Configuration Protocol (DHCP) (RFC 2131)	UDP	67/ 68	Used on networks that do not use static IP address assignment (almost all of them). Can be set up with a poll of addresses that are available for assignment. When a client device is turned on it can request an IP address from the local DHCP server, if there is an available address in the pool it can be assigned to the device. This assignment is not permanent and expires at a configurable interval; if an address renewal is not requested and the lease expires the address will be put back into the poll for assignment.
Trivial File Transfer Protocol (TFTP) (RFC 1350)	UDP	69	TFTP offers a method of file transfer without the session establishment requirements that FTP uses. Because TFTP uses UDP instead of TCP it has no way of ensuring the file has been properly transferred, the end device must be able to check the file to ensure proper transfer. TFTP is typically used by devices to upgrade software and firmware; this includes Cisco and other network vendors' equipment.
Hypertext Transfer Protocol (HTTP) (RFC 2616)	TCP	80	Commonly used protocols on most networks. HTTP is the main protocol that is used by web browsers and is thus used by any client that uses files located on these servers.
Post Office Protocol (POP) version 3 (RFC 1939)	TCP	110	POP version 3 is one of the two main protocols used to retrieve mail from a server. POP was designed to be very simple by allowing a client to retrieve the complete contents of a server mailbox and then deleting the contents from the server.
Network Time Protocol (NTP) (RFC 5905)	UDP	123	Used to synchronize the devices on the Internet. Even most modern operating systems support NTP as a basis for keeping an accurate clock. The use of NTP is vital on networking systems as it provides an ability to easily interrelate troubles from one device to another as the clocks are precisely accurate.
NetBIOS (RFC 1001-1002)	TCP/UD P	137/138 /139	Not a protocol but used in combination with IP with the NetBIOS over TCP/IP (NBT) protocol. NBT has long been the central protocol used to interconnect Microsoft Windows machines.
Internet Message Access Protocol (IMAP) (RFC 3501)	TCP	143	IMAP version3 is the second of the main protocols used to retrieve mail from a server. While POP has wider support, IMAP supports a wider array of remote mailbox operations which can be helpful to users.
Simple Network Management Protocol (SNMP) (RFC 1901-1908, 3411-3418)	TCP/UD P	161/162	Method of network management. Many abilities: ability to monitor, configure and control network devices. SNMP traps can be configured on network devices to notify a central server when specific actions are occurring. These are used when an alerting condition is happening: the device will send a trap to network management stating that an event has occurred and that the device should look for a source to the event.
Border Gateway Protocol (BGP) (RFC 4271)	TCP	179	BGP version 4 is widely used on the public internet and by Internet Service Providers (ISP) to maintain very large routing tables and traffic processing. BGP is one of the few protocols that have been designed to deal with the astronomically large routing tables that must exist on the public Internet.
Lightweight Directory Access Protocol (LDAP) (RFC 4510)	TCP/UD P	389	LDAP provides a mechanism of accessing and maintaining distributed directory information. LDAP is based on the ITU-T X.500 standard but has been simplified and altered to work over TCP/IP networks.
Hypertext Transfer Protocol over SSL/TLS (HTTPS) (RFC 2818)	TCP	443	HTTPS is used in conjunction with HTTP to provide the same services but doing it using a secure connection which is provided by either SSL or TLS.
Lightweight Directory Access Protocol over TLS/SSL (LDAPS) (RFC 4513)	TCP/UD P	636	Just like HTTPS, LDAPS provides the same function as LDAP but over a secure connection which is provided by either SSL or TLS.
FTP over TLS/SSL (RFC 4217)	TCP	989/990	Again, just like the previous two entries, FTP over TLS/SSL uses the FTP protocol which is then secured using either SSL or TLS.

INTERVIEW

ANECDOTES

Fred Kavli, NTH Physics, Kavli foundation for astrophysics, nano-sciences, neurosciences – CDS of AIDC more +ve than BHP

Portfolio

12+ strategy process change projects at CIBC, SCOTIA, AIG and for Price Waterhouse: 5 vendor-solution implementation + 5 outsourcing + 2 development projects (from vendor)
Jul14: IT Best Practices & Mentoring CBOC LITCOM
Apr14: Lead Engagement ALGORITHMICS, NCB EVOQ
Oct13: Scotia Bank NFF, Collection System Replacement, Retail loan, Family of Cards
May13: Control Solutions AGNICO-Eagles Mines JD Edward, IT Ops consolidation
Nov10: HOOPP Back office automation, Upgrade, Methodology
Jun09: CIBC Risk Strategic Initiatives RSI (CAD 80M)
Jan07: SIERRA
◆Jan09: (Sierra) MANULIFE Der. Actng GAAP "Other Than Temporary Impaired" (OTTI) ◆Jun08: (Sierra) CIBC – SOX Secure End User Computing SEUC (Middle, ***Wealth***) ◆Jan07: (Sierra) CIBC Mellon Fin Sys Renewal Project FSRP Treasury, BI/MIS/DW ◆Oct07: (Rescue) Balanced Scorecard/BI BC Corp Acctng Services (public sector), ◆Jan08: (Rescue) Russell-Mellon Enterprise Investment Platform (***Wealth***) ◆Mar08: (Rescue) MTO Road User Safety Revenue Mgt System (public sector) ◆Jan09: (Rescue) Travel Insurance Coordinators TIC merges Trent Health
Mar05: CIBC – Internal Control Repository (CAD 20M)
Nov00: XEG - SME, State organizations
Jun96: AIG – PMO set up, Harvester, India, VN, China (USD 100M)
Oct93: AIDC - Treasury system, financial repository (AUD 5M fee income)
Oct90: PWU WESTPAC DCPK Front/back office for FOREX (AUD 3M)
Aug86: ND COMTEC - integrated graphic system revenue (CAD 2M)
Aug84: ESSO Exploration (DB of 20 North Sea fields 200K barrels oil equivalent per day)

Interview Techniques

REMEMBER SMILE - EYE CONTACT - CONNECT - CLARIFY - REFLECT - REPEAT - BE SILENT - EMPATHISE - PHYS. DISTANCE - I-STATEMENT - HOWEVER, MY FORMER - THANK YOU "I hope we'll have the opportunity to work together in the future" **SAR** •Situation •Action required to find solution •Share Result **STAR** (Interview) = Situation, Task, Action, Result - *what is the problem, what did i do, who did i talk to, how did i do that, how do i know that it was well done – focus on last 3 good projects* - **RAID** (Risk) = Risk, assumption, issue, dependency - **BOSCARD** (Charter) = Background, opportunity, scope, constraints, assumptions, risks, deliverables - **BATNA** – **INVEST** (change request) = independent, negotiable, valuable, estimatable, small, testable **– SMART** (goals) = specific, measurable, attainable, relevant, timely

Top 5 things in next job

❶Satisfaction ❷Advancement ❸Location ❹Management Culture ❺Pay

Dialogue General

8 behaviors in team and individual assessments

❶Express authentic appreciation ❷Address shared interest ❸Appropriately include others ❹Keep all your agreements ❺Express reality-based optimism ❻Be 100% committed ❼Avoid blaming and complaining ❽Clarify roles, accountability and authority

How to succeed?

Define using other party's languages -Communicate understanding -Get confirmation -State objectives -Set communication channels: steering committee, forum, email, telephone, project plan -Dedicated team with specific/strategic tasks –Plan, allocate resources (20% high potential, 40% strategic, 30% core, 10% support) -Customer feedback –SLA

AGILE AUDIT

Agile concepts: •Audit Increment planning" build a backlog of key risks and controls •Execute each sprint (2 week intervals) •After each sprint have a sprint review meeting with L4 to discuss results and initiate. After each sprint have tollgate to discuss stopping or continuing with audit •After each sprint and before next Sprint have Lessons learned session to discuss went well in sprint and what needs enhancements from next sprint •Holding daily scrum meetings (10 minutes) to discuss progress from yesterday, plan for current day and if any escalation is required

AUDIT SAP

SAP R/3 REVENUE BUSINESS CYCLE • Master Data Maintenance • Sales Order Processing • Shipping, Invoicing, Returns and Adjustments • Collecting and Processing Cash Receipts	**AUDITING SAP R/3 REVENUE BUSINESS CYCLE** • Master Data Maintenance • Sales Order Processing • Shipping, Invoicing, Returns and Adjustments • Collecting and Processing Cash Receipts
SAP R/3 EXPENDITURE BUSINESS CYCLE • Master Data Maintenance • Purchasing • Invoice Processing • Processing Disbursements	**AUDITING SAP R/3 EXPENDITURE BUSINESS CYCLE** • Master Data Maintenance • Purchasing • Invoice • Processing Disbursements • Testing Techniques
SAP R/3 INVENTORY BUSINESS CYCLE • Master Data Maintenance • Raw Materials Management • Producing and Costing Inventory • Handling and Shipping Finished Goods	**AUDITING SAP R/3 INVENTORY BUSINESS CYCLE** • Master Data Maintenance • Raw Materials Management • Producing and Costing Inventory • Handling and Shipping Finished Goods
SAP R/3 BASIS APPLICATION AND TECHNICAL INFRASTRUCTURE • SAP R/3 Architecture • SAP R/3 Basis Application Infrastructure • Audit Implications	**AUDITING SAP R/3 BASIS APPLICATION INFRASTRUCTURE** • Installation Management Guide • Organization Model

	• Critical Number Ranges • Modifying Critical Tables • ABAP/4 Workbench/ Transport System • Customizing and Executing ABAP/4 Programs • ABAP/4 Development in Production • Data Dictionary Changes • Queries Company Code Setting • Computer Center Management System • Profile Generator and Security Administration • Case Study

Conflict with a co-worker

STAR=Situation– Continuity report for finance report due for end of the year Reluctant co-worker **Task** Feasibility Budget **Action** Clarify requirements, work schedule **Result** Split report, Off-load analysis, testing - *I sat down with my co-worker at company x and asked what her issues were. Then I stated my concerns. We both discussed our most important issues and the ones we could compromise on. Once we identified and prioritized common goals, we decided together what to give up and what to keep. Both of us felt like we were gaining something and were instrumental in the compromise*

1 How do you rescue program/projects?

The first steps I took ❶**Management level assessment** ◆Sponsor, internal stakeholders and management say about the situation (**Diligence of eliciting requirements** Establish communication update plan for assessment period ❷**On the ground assessment** Unwind where the project is vs. where it should be - Ask for people thoughts on what is wrong ❸**Update stakeholders** ❹**Present plan based on assessment** **Project failure causes** ❶**Poor Change Management** scope creep ❷**Poor Communications** → Communication plan ❸**Inadequate Resources** not committed resources, lack of support, no analysis and documentation of skill sets, conflicting resource delegation, turnover, dependence on heroes ❹**Poor Requirements** ambiguous priorities, imprecise information ❺**Poor Planning** Inaccurate Estimates, unrealistic timetable, missing key processes, poor estimates/ data ❻**Poor Risk Management** ❼**Poorly Defined Deliverables** ❽**Over Optimism** ❾**No Time for Project Management** ❿**Poor PM skill** **Rescue steps** ❶Improve stakeholder's communications (what to expect) ❷Re-evaluate resources ❸Refine project & scope ❹Use right technology ❺Replace PM 🕮Project Audit 🕮Risk Management

2-1 Senior stakeholders with different opinion

❶Know senior management requirements (put themselves in boss's shoes, be sympathetic to challenges, problems, and pressures of senior managers) ❷Analyze boss's thinking patterns, act in ways that are consistent with that pattern (analytically or intuitively) ❸Listen, look for verbal and nonverbal components of boss's message, just as a project ❹Take solutions as well as problems to boss & explore alternatives & make recommendations ❺Keep boss informed of progress and plans ⇨ boss can act as a mentor, give support ❻**Consult boss on policy procedures & criteria** help clarify management philosophy & establish boundaries related to administrative issues (to protect oneself) ❼**Avoid steamrolling** boss; be patient, allow time for thinking & evaluation will lead to better relationships and results

Managing Up ◆Maintain Energy And Maximize Efficiency ◆Being fully effective springs from building a reputation for being a *team player*, demonstrating a willingness to *accept responsibility*, bringing *new ideas to the job*, and being *productive* ◆Managing is not the exclusive property of MBA graduates ◆At times we are all managers, and we are all support staff ◆Those who manage up have to think - and act -like managers ◆A good manager is a student of cause and effect ◆It's not good enough to be aware of what's happening around you; you must also know why it is happening ◆If you are not helping, you are hindering ◆Ask yourself: Did the work I performed today help achieve a goal?

Meetings Project meetings ◆COBIT Governance & Management ◆

2-2 Handle conflicts

◆**Set framework** (*stakeholder map*, *roles & responsibilities*, *communication plan*, *issue resolution*, *change management*, *risk management*) to communicate the options, the pre-requisites and the implications in a simple, structured and clear in order to reach a consensus-based pragmatic solution ◆**3 types of conflicts** ①**Goal-oriented conflicts** (associated with end results, performance specifications & criteria, priorities, objectives) CIBC-M Finance-Treasury, SCOTIA BA/Architect ②**Administrative conflicts** (management structure, roles & reporting relationships, responsibilities & authority for tasks, functions, decisions, budget & cost, hr, schedule) CIBC RSI Staffing, Budget, Requirements, SOX Performance ③**Interpersonal conflicts** (differences in work ethics, styles, egos, personalities of participants) ◆**Resolutions** Conflict over ❶**Project priorities** (sequence of activities & tasks, goals incompatibility & differences in long-term/short-term) ⇨ Master plan compatible with long-term strategies ❷**Administration procedures** ⇨ Clarify roles, responsibilities, reporting relationships at project start ❸**Technical opinions & performance trade-offs** ⇨ Peer review & steering committees to review specifications & design ❹**Human resources, staffing, allocation/hiring project personnel)** ⇨ Work breakdown structure ✚ responsibility matrix ❺**Cost & budget** ⇨ Budgets supported by detailed budget and cost estimates of subproject tasks & activities ❻**Schedules** ⇨ schedule integrating schedules for subprojects with staffing & other life constraints ❼**Personality** ⇨ Emphasize team building, create environment emphasizing respect, diversity, and equality See 14. *How do you resolve*

2-3 Negotiation techniques

◆**BATNA** (both parties alternatives & resistance point) - Prepare & plan, Subject knowledge, Patience & Listen ◆**Principled negotiation** •**Positions**: one party's (usually self-serving) solution to problem •**Issues**: elements/ subject matter of dispute to be negotiated •**Interest**: factors motivating parties to reach respective positions and underlying foundation for positions, including desires and concerns

2-4 Building blocks for Stakeholder management

3-1 What is your management style?

3-2 What makes you a world-class leader?

Consultative, professional, respectual, hands-on, persistent

4 Challenges of migration projects, e.g. M&A projects?

❶Familiarize with new environment ❷Determine correct migration, upgrade path ❸Determine new environment requirements (resources, system) ❹Plan testing ❺Allow time for performance tuning ❻Set up training environment ❼Plan for backup & recovery

5 How do you hold team members accountable?

❶Handbook (scope, procedures) ❷Clear role ❸Measurable performance criteria ❹Meeting, communication

6 How do you handle unhappy stakeholders or clients?

❶Involve stakeholder in prioritization of requirements ❷Ensure business sign-off of charter and requirements ❸Ensure minimum weekly face-to-face meeting on progress ❹Invite business to (some) project status meeting

7 How do you handle excessive work demand?

❶Acknowledge team extra effort ❷Inform business of related risk ❸Review risk log and approach to remedy ❹Review plan/workflow to identify bottleneck

8 What do you think challenge you in this position?

❶Engage stakeholder ❷Optimize team performance ❸Detect/ correct problems on time

9 How do you handle very poorly performing project staff?

❶Diagnose poor performance ❷Enhance ability (Resupply, Retrain, Refit, Reassign, Release) ❸Improve motivation (performance goals, assistance, feedback)

10 Your 3 recommendations to manage PMO?

❶Engage stakeholder ❷Optimize team performance ❸Continuous improvement

11 How do you motivate?

❶Be realistic and specific ❷Create a safe environment (shield from org politics) ❸Be a role model ❹Know the team members ❺Recognize effort, progress, contributions ❻Celebrate ❼Empower ❽Link project success to corporate strategy – Get recognition from senior management

12 How do you negotiate?

❶Know your opponent ❷Know the subject to negotiate ❸Know your BATNA

13 Leading organizational change management

…on projects whose benefits relied significantly on high degree of behavioral changes

Change Management

❶Shared understanding of reality of change ❷Formulate the change ❸Plan the change ❹Implement the change ❺Manage change transition ❻Sustain change

Promoting Behavior Changes

❶Increase benefits ❷Decrease costs ❸Decrease the desirability of competing alternatives ❹Socially Desirable ❺Easily Done ❻Seek Sr. Management blessing

Types of Resistance to changes

❶**Technical resistance** ①**Habit & Inertia** (bureaucratic traditions vs. new ways) ②**Fear of the Unknown** ③**Prior investment** (fear of waste)

❷**Political resistance** ①**Resource allocation** (doing more with less) ②**Leaders indictment** (full responsibility over the overloading of market risk system) ③**Threats to powerful coalitions** (C-M Operations & IT)

❸**Cultural resistance** ①**Old cultural mindsets** (CIBC/HOOPP gung-ho trading, AIG dominance) ②**Sense of security** ③**Climate for change** (pension not in the crosshairs)

🕮Fighting Resistances to Changes 🕮Change Management in Portfolio, Program, Project 🕮Organizational Project Management (OPM3) 🕮Change Management at Portfolio Level 🕮Change Management at Program Level 🕮Change Management at Project Level

14 How do you resolve personal conflict?

❶Be neutral third party ❷Establish rules of conduct ❸Meet both parties in calm & controlled setting ❹Control discussion ❺Understand perspectives ❻Reach working solution ❼Status Quo unacceptable

15 How do you create alignment among partners?

❶Create stakeholder matrix ❷Seek common understanding of project objectives (Project Charter) ❸Define detailed RACI chart ❹Ensure representation within the team ❺Ensure adequate communication plan

16 How do you manage stakeholders?

❶Identify ❷Prioritize ❸Understand their needs ❹Engage ❺Monitor engagement - Report project health

17 How I support new staff?

Program/project handbook ❶Program Scope ❷Program Approach ❸Program Management, Control Process ❹High Level Program Plan ❺Project Governance ❻Change Management ❼Roles & Responsibilities ❽Weekly Status Report Process ❾Centralized Issues Log ❿Project Control Mechanism

18 What I did when I screwed up?

❶Assess the damage ❷Admit your mistake immediately ❸Be direct and unambiguous ❹Take responsibility with humility ❺Take a step back and breathe ❻Don't throw others under the bus ❼Devise an action plan ❽Do everything in your control to make it right ❾Prepare yourself for the consequences ❿Don't be too hard on yourself

19 What did you do when the project is behind schedule?

❶Work overtime ❷Reallocate resources (critical path) ❸Double-check dependencies ❹Check time-constrained activities (sign-off, training) ❺Swap resources ❻Crash schedule (increase resources) ❼Fast track it (make sequential partially or totally parallel) ❽Prevent all scope change ❾Improve processes ❿Scale back the scope of work

20 What did you do when the project is over budget?

❶Work unpaid overtime ❷Swap human resources ❸Eliminate or replace non-labor costs ❹"Zero tolerance" scope change ❺Use budget contingency ❻Scope back the work

21 Basic Requirements for controlling project

❶**Plan** (realistic, credible, detailed enough to be executed, acceptable to those who must execute it, approved by those who are accountable (SRO/ Project Board) ❷**Process for monitoring/ managing** progress & resource usage ❸**PM organisation** (skilled people with sufficient authority & time to plan, monitor, report, take decisions & deal with exceptions ❹**Process for minor corrections & adjustments** (minor deviations & omissions) ❺**Commitment** to provide resources (SRO, Project Board, Stakeholders, resource 'owners') ❻**Explicit authority** to proceed by accountable (SRO/ Project Board)

22 Auditing Projects

Software architecture audit model

Architecture	Security	Tools
◆Application architecture ◆Database architecture ◆Overall architecture	◆Application security ◆Web service security ◆Database security	◆NET framework ◆Visual Studio ◆3rd party
Process	**Efficiency**	**Performance**
◆Code management ◆Quality control ◆Methodology	◆Libraries ◆Frameworks ◆Factories	◆Availability ◆Maintainability ◆Scalability

Project Lifecycle Documents (10)

❶Feasibility Study ❷Specification ❸Cost effectiveness Analysis ❹Project Integration ❺Requirements ❻Internal Control ❼Testing ❽User Acceptance ❾Final Assessment ❿Project Context

Feasibility Study (5)	*Specifications (7)*	*Cost Effectiveness Analysis (4)*	*Project Integration (5)*	*Requirements (4)*
❶Objectives ❷Solutions ①System demands ②Solutions (variants) ③Costs, risks, advantages **❸Resources/ Funding** (demands on project & organisation) **❹Feasibility ❺Readiness** (can concept phase begin/ project commissioning)	**❶Objectives ❷Expectations** (users, stakeholders) **❸Functionalities ❹As-Is** (what available) **❺Project size ❻Project constraints ❼Technology requirements**	**❶Total costs** (e.g. operational costs of data migration, capacity, training **❷Assessed use for quantity, quality ❸Project cost effectiveness**	**❶Integration** (corporate strategy + IT structures) **❷Project overlap ❸Synergy ❹Conform to standards ❺Automatic/ manual interfaces**	**❶Internal** (agreements, procedures, quality norms) **❷External** (laws, regulations, directives, contracts) **❸Specificity** (data protection, publication, procurement procedures, banks, best practices) **❹Effect on processes/ infrastructure** (architecture, security)
Internal Control (4)	*Testing (5)*	*User Acceptance (5)*	*Final Assessment (5)*	*Project Context (4)*
❶Automatic controls (data input validity check, automatic comparisons, error lists) **❷Functions to be separated/ access permission ❸Measures to control ❹Measures for continuity in operations** (emergency plan)/ **preservation of data** (archive plan)	**❶Purpose ❷Plan** (methods, tools, criteria, case studies) **❸Resources** (availability, time constraints **❹Test methods ❺Test results**	**❶Acceptance definition ❷Data/ application ownership ❸UAT signoff ❹Test cases ❺Acceptance conditions**	**❶Objectives achieved & requirements fulfilled ❷Final cost & variances ❸Cost effectiveness calculation ❹Post-implementation risk ❺Lessons learned**	**❶Extensive user involvement ❷Performance appraisal ❸Extent of standardisation ❹Quality assurance systems & procedures**

Project Survival Test

REQUIREMENTS	PLANNING	PROJECT CONTROL	RISK MANAGEMENT	PERSONNEL
❶Clear, unambiguous **vision/ mission statement** ❷Realistic vision ❸**Business case** with business benefit and benefit metrics ❹**User interface prototype** to demonstrate functionality ❺Detailed, written **specification** ❻Did the project team interview people who will actually use the software (end users) early in the project and continue to involve them throughout the project?	❶Detailed, written **Software Development Plan** ❷**Project task list** include creation of an installation program, conversion of data from previous versions of the system, integration with third-party software, meetings with the customer, and other "minor" tasks ❸**Schedule and budget** estimates officially updated ❹Detailed, written **architecture and design** documents ❺Detailed, written Quality Assurance Plan that requires design and code reviews in addition to system testing ❻Detailed **Staged Delivery Plan** for implementation & delivery ❼**Project plan** include time for holidays, vacation days, sick days, and ongoing training, and are resources allocated at less than 100% ❽**Project plan & schedule** approved by development, quality assurance, technical writing	❶Single key **executive** with decision-making authority ❷Project manager's **workload** adequate ❸Well-defined, detailed **milestones** ("binary milestones" 100% done or not done) ❹Published **milestones** with status ❺**Feedback channel** for anonymous report of problems ❻**Change management plan** ❼**Change Control Board** with authority to accept or reject proposed changes ❽Published **planning materials, status information** including effort, schedule estimates, task assignments, progress compared to the plan thus far available to every team member ❾Automated **revision control** ❿Defect tracking software, source code control, PM software	❶List of current risks to project ❷List updated frequently ❸**Project risk officer** to identify emerging risks ❹Plan for managing subcontractors	❶Team technical expertise ❷Expertise with business environment in which the software will operate ❸Technical leader capable of leading project successfully ❹Enough people to do all the work required ❺Everyone work well together ❻Each person committed to the project

23 SDLC

❶**Preliminary Analysis** organization's objectives, nature & scope of problem under study - alternative solutions - costs & benefits - preliminary plan with recommendations ❷**Systems analysis**, **requirements definition** project goals defined into functions/ operation of application - end-user information needs ❸**Systems design** features & operations in detail (screen layouts, business rules, process diagrams, pseudo-code, etc.) ❹**Development** Code writing, Integration & testing ❺**Acceptance, Installation, Deployment** ❻**Maintenance** changes, correction, additions, moves to different platforms, etc.

DELIVERABLES ❶**Requirements Management** change control ❷**Development Approach** SW development plan/project charter, development case/process plan, iteration plan/phase ❸**Issue Management/ Change Control** effort ✚ cost impact of change ✚ recommended solution ❹**Risk Management** identify, analyze, prioritize, identify risks (mitigate/retire early high risks, use requirements confirmation to mitigate scope/functional risk, architectural POC to eliminate technology risk) ❺**Quality Management** quality planning, assurance & control ❻**Configuration Management** evaluate, coordinate, approve/disapprove, implement changes in artifacts used to construct & maintain SW ⇨ define •set of artifacts (configuration items) under CM jurisdiction •naming of artifacts •entry/exit of controlled set •change rule •availability for use rule •CM tools ❼**Test Management** test strategy & plan ❽**Project Acceptance** user acceptance process & sign-off ❾**Project Closeout**

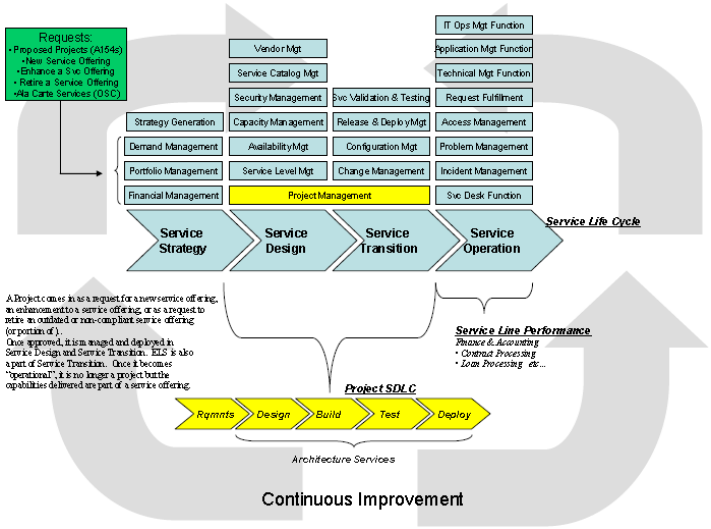
36 Deliverables subject to Change Control

❶Change Control Plan ❷Change Proposals ❸Vision statement ❹Top 10 Risks ❺SW Development Plan (project cost, schedule estimates)	❻User Interface Prototype ❼User Interface Style Guide ❽User Manual/ Requirements Specification ❾Quality Assurance Plan ❿SW Architecture	❶SW Integration Procedure ❷Staged Delivery Plan ❸Individual Stage Plans (miniature milestone schedules) ❹Coding Standard ❺SW test cases	❻Source code ❼Media (graphics, sound, video) ❽SW build instructions make files ❾Detailed Design Document per stage ❿SW Construction Plan for each stage	❶Install program ❷Deployment (Cutover Handbook) ❸Release Checklist ❹Release Sign-Off Form ❺SW Project Log ❻SW Project History Document
❶Change Control Plan ❷Change Proposals ❸Vision statement ❹Top 10 Risks ❺SW Development Plan (project cost, schedule estimates)	❻User Interface Prototype ❼User Interface Style Guide ❽User Manual/ Requirements Specification ❾Quality Assurance Plan ❿SW Architecture	❶SW Integration Procedure ❷Staged Delivery Plan ❸Individual Stage Plans (miniature milestone schedules) ❹Coding Standard ❺SW test cases	❻Source code ❼Media (graphics, sound, video) ❽SW build instructions make files ❾Detailed Design Document per stage ❿SW Construction Plan for each stage	❶Install program ❷Deployment (Cutover Handbook) ❸Release Checklist ❹Release Sign-Off Form ❺SW Project Log ❻SW Project History Document

24 Project Management Transition

❶Project kick-off presentation deck review **❷Project schedule** deep dive **❸Project finance** deep dive **❹Project Culture ❺Project Staffing ❻Project stakeholders & interests ❼Assistance** (further)

25 Project Management and ITIL



◆**PM = Service offering** ◆**Project = service request** (ITIL *Change Management*) ⇨ ***approved, designed, managed, deployed*** (ITIL *Service Design, Transition*) 🕮**ITIL Change Management** (❶Record RFC ❷Review RFC ❸Assess & Evaluate RFC ❹Authorize RFC ❺Plan ❻Implement & Coordinate ❼Review & Close) 🕮**ITIL Service Design** (❶Service Catalogue Management ❷Service Level Management ❸Capacity Management ❹Availability Management ❺IT Service Continuity Management ❻Information Security Management ❼Supplier Management) 🕮**ITIL Service Transition** (❶Change Management ❷Service Asset & Configuration Management ❸Release & Deployment Management ❹Minor Service Transition Processes)

26 Program Management

🕮**Program Management Process (Ricardo Vargas)** **DEFINITION – BENEFITS DELIVERY – CLOSURE** and **9 Competencies** ❶Communication ❷Financial ❸Integration ❹Procurement ❺Quality ❻ Resource ❼Risk ❽Schedule ❾Scope
🕮**Program Life Cycle (5)** ❶Pre-program setup ❷Program setup ❸Program Mgt & Technical I/F ❹Benefit delivery ❺Program closure
🕮**Project Selection Criteria (9)** ❶Strategic alignment ❷ROI ❸Expected benefits ❹Urgency/ market reactive ❺Project type (new, maintenance) ❻Dependency with major project/program ❼Risk factor ❽Time to complete ❾Complexity

27 Portfolio Management

🕮**Portfolio Management principles & practices (10)**
❶Strategic focus ❷Strategic initiatives ❸Portfolio Components ❹Quantifiable Components ❺Time Horizon ❻Portfolio snapshot ❼Portfolio Management Activities ❽Alignment to Organization Strategy ❾Governance ❿Balancing of conflicting demands
🕮**Portfolio Management Process Groups (5)**
❶Strategic ❷Governance ❸Performance ❹Communication ❺Risk
🕮**Portfolio Management Tools & Techniques (4)**
❶Analysis ❷Selection ❸ Meeting ❹Communication
Analysis (15) ❶Strategic alignment ❷Prioritization ❸Scenario ❹Capability & Capacity ❺Interdependency ❻Cost/benefit ❼Stakeholder ❽Readiness ❾Portfolio Organizational Structure ❿Graphical Analytical Tools ❶Quantitative & Qualitative ❷Value Scoring & Measurement ❸Benefits Realization ❹Communication Requirements ❺Gap **Selection (4)** ❶Portfolio component inventory ❷ Portfolio component categorization ❸Weighted ranking & scoring ❹Portfolio authorization **Meeting (1)** ❶Portfolio review meetings **Communication (4)** ❶Communication methods ❷Elicitation techniques ❸Portfolio Management information system ❹Integration Portfolio Management

28 Contract Management

Areas (7) ❶Authoring & negotiation ❷Baseline management ❸Commitment management ❹Communication management ❺Contract visibility & awareness ❻Document management ❼Growth **Contract Placement Stages (4)** ❶Requirements Analysis ❷Evaluation Plan ❸Invitation to Tender ❹Proposal Evaluation **Contract Management phases (5)** ❶Initial ❷Bid ❸Development ❹Manage ❺Maintenance

29 Architecture

🕮**TOGAF** 🕮**ZACHMAN** 🕮**NET** 🕮**Mobile** 🕮**Data Architecture** 🕮**Service architecture** 🕮**LIFE architecture** 🕮**Risk Architecture** 🕮**SCOTIA NFF** 🕮**SCOTIA Direct Loan** 🕮**MTO Revenue**

30 DATA management

🕮**BCBS 239 (BASEL III) Requirements** 🕮**Risk Data 7 Areas 400 Requirements** 🕮 **20 Key Risk Reports** 🕮**20 Conceptual Data Models** 🕮**20 Key Risk groups data feeds** 🕮**8 Key Risk groups Data** 🕮**Risk Case Studies** 🕮**Risk Architecture** 🕮**SUNGARD** 🕮**CVA data requirements** 🕮**CIBC Risk** 🕮**Risk Topics** 🕮**Lexicon Risk** 🕮**DARPA Data Management** **11 Knowledge Areas**

Data Issue resolution

◆**Data integrity** (resulting in inefficiency/costly rework, concerns over data shared with/ received from 3rd parties, excessive customer complaints or disputes) ◆**Management information** for effective decisions ◆**Significant data conversion, integration/ data cleansing** activities ◆Potential overpayments/ revenue leakage issues ◆**Complex spreadsheet models** support key business decisions ◆**End-User Computing (EUC)** not supported by IT ◆**Lack of internal skill set / capacity** to perform electronic data analytics and testing of complex business logic on a periodic bases

Merits of ETL and ELT

ETL extract-transform-load means risk is always playing catch-up **ELT extract-load-transform** continuous change and adaptation, less needs to predict exactly how information is used in the future

Credit scorecard development

❶**Data cleansing a-**Missing values/ outliers **b-**Correlation of financial characteristics **c-**Determine strength of financial characteristics **d-**Intuitive application (business / operational considerations)) ❷**Variable selection** (final set of characteristics 5 to 10) apart from other information like borrower's name, default information (# days past due) ❸**Scorecard development** ❹**Validation**

Data Quality Management Project example

❶Establish DQM environment ❷Scope project & implementation plan ❸Implement DQM project (define, measure, analyze, improve) ❹Evaluate DQM project

31 Best Practices and Standards

◆*Business Continuity* COBIT, ISO 27002, Business Continuity Institute (BCI) ◆*IT Governance* COBIT◆*Information security management system (ISMS)* ISO 27000, SANS Top 20 security controls

32 RFI/RFP

10+ years selecting / managing vendors, issuing RFP, conducting Proof-of-Concept and negotiating contract for 4 enterprise initiatives of up to $80M at CIBC, CIBC Mellon and AIG RFQ, RFP, contract negotiation, SLA, Statement of Work, vendor performance monitoring (in development and production) - **CIBC RSI 2009** ($80M project $35M annual, Industry Scan, RFP, POC, Contract) **CIBC EUC 2008** ($3M, Industry Scan, RFI, POC, Contract) **CIBC Mellon 2007** ($3M, Industry Scan, RFP) **AIG India Vietnam 1999**
Phases (6-8 months) Scope (1 month) Preparation (1 month) RFP (2.3 months - Vendor contact 3 weeks, Vendor demo 2 weeks, Vendor Follow-up 2 weeks, Scoring/selection 2 weeks) Contract (2 months) 🕮**Vendor Selection Toolkit**

33 Service Management, ITIL, IT Governance

ITIL, COBIT capabilities ◆Implement KPIs with Balanced Scorecard (financial, customer, learning & growth, internal operations) ◆Continual improvement ◆Incident mgt ◆Problem mgt ◆Change mgt ◆Configuration management ◆Operational governance 🕮 (COBIT) ◆🕮SLA ◆OLA ◆Change advisory board ◆Steering committee ◆Known error database ◆AGNICO (May – Oct13) ◆HOOPP (Dec10 – Feb11) 🕮ITIL Service Delivery processes 🕮ITIL Infrastructure 🕮ITIL Strategic questions 🕮Lifecycle of Service Continuity Management 🕮Resource Management Infrastructure 🕮COBIT 4 domains 🕮COBIT Components 🕮COBIT Domains and Processes

40 Other PM topics in this document

➢Leading and mentoring ➢Estimation techniques ➢Gathering business requirements ➢Process analysis ➢Managing timelines ➢Conducting technical reviews ➢Development of Quality Management, Change Management, Issues & Risk Management plans, Communication plan, Project Charter ➢Change requests ➢Gating ➢Project governance

41 Techniques to manage timelines

❶**Detailed planning** (for 3-4 months ahead, up to 7-8 level deep of work breakdown structure) ❷Well-defined **milestones with ownerships** ❸Daily **review of risks and threats** ❹Visual **reports of project progress- challenges** ❺**Contingency planning** and **risk management planning**

42 Techniques in conducting project meetings

Agenda to plan project ❶Welcome ❷Review Project Charter & Mission Statement ❸Project Scope ❹Major milestones ❺Task List and Dependencies ❻Risks and Mitigation Strategies ❼Project Communications ❽Information Repository ❾Action Plans

Various types of project meetings

◆**Steering Committee for governance**, **project status Mthly** (HOOPP – CIBC) ◆**Executive Committee for project status Wkly** (HOOPP – CIBC) ◆**Project team meeting** for status, issue resolution – **Change management meeting** – all projects

43 Techniques to conduct technical reviews

❶**Formulation of key questions** with the help of SMEs ❷Construction of "**evidence map**" to delimit areas for review ❸**Critical appraisal** with checklist, quality scales ❹**Audit trail** from business requirements to technical solutions ❺**Meetings and workshops management** with clear agendas, minutes and action plans

44 Issues & Risk Management

For each **risk type** (organization specific, project specific, policies and procedures, technology, etc.), Identify and document the risk description, mitigation approach, contingency plan, likelihood of occurring, potential impact ($ / schedule / quality etc)

RAID ❶**Risks** = combined likelihood the event will occur and impact on - includes description, full analysis and plan to manage❷**Assumptions** factors assumed to be in place that will contribute to the successful result of project - includes details of the assumption, the reason it is assumed and the action needed to confirm whether the assumption is valid ❸**Issues** something going wrong – includes description, impact, seriousness and actions needed to contain and remove ❹**Dependencies** event/ work dependent on result of project, or your project will depend on - captures who you are dependent on, what they should deliver and when, who is dependent on you

45 Quality assurance

Tools benchmarking, benefit/cost analysis, walkthroughs, audits •**Reviews** process, objectives, schedule, board/ action team, responsibilities

46 Quality Management

For each phase (*initiation, planning, control/ execution, closing*), define the quality requirements and activities for the related deliverables and activities

❶ Quality Activities

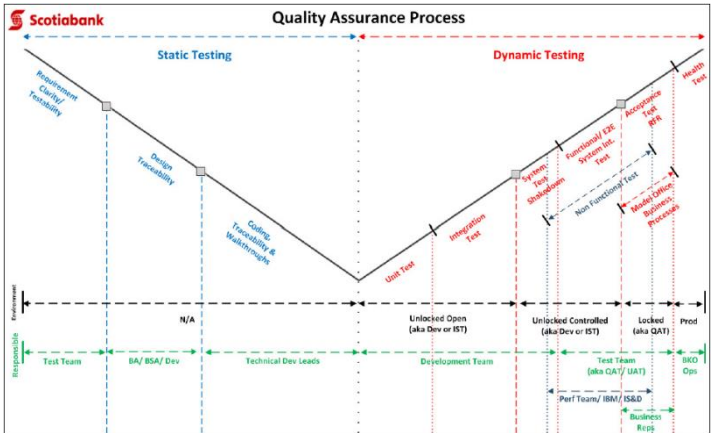
Deliverable/Activity	Quality Activity	Comments
Initiation & requirements, design, construction, testing, implementation		

❷ Standards and Guidelines

Standard	Owner & Location	Description	Exemption

•Data quality management •AGILE quality

47 Quality processes in SDLC Phases



48 Communication Plan

- I can get requirements for the communication Deliverable; identify the Producer, Receiver, Frequency and the Medium

📖Communication Plan 📖Engagement/Communication Plan Structure

49 Project charter

- Key sections - project definition, business need and justification, in-scope, out-of-scope, key deliverables, tentative schedules, risks and challenges, project governance, project manager, key staff and stakeholders
- BOSCARD ❶**Background** (motivation, key stakeholders) ❷**Objectives** (goals linked to SMART objectives) ❸**Scope** (features/ functions of product, result) ❹**Constraints** (limits, conditions on scope) ❺**Assumptions** (for planning, to be validated) ❻**Risks** (with quick assessment of significance and mitigation) ❼**Deliverables**

50 Techniques to estimate change requests

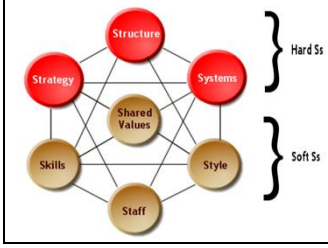
❶Itemized changes **INVEST** (Independent, Negotiable, Valuable, Estimatable, Small, Testable) ❷Inclusive of **all aspects of delivery** (analysis, design, implementation, testing, refactoring, deployment) ❸**Input from all concerned parties** including business, project team, IT ❹**Estimation methods**: affinity, wideband Delphi, ideal time, relative sizing based on experiences and history ❺ITIL Incident, problem, change

Techniques to negotiate change requests

•Itemized changes INVEST •Min. 3 alternative choices of implementation •Ranking based on business value and priority combined with Technology risk and difficulties •Collective understanding of impact on project (time, resources and cost) •BATNA (Best Alternative to Negotiated Agreement) •Active listening •Facilitation

51 Business requirements

Situation	Task	Action	Result



McKinsey way

MECE = Mutually Exclusive, Collectively Exhaustive

80/20 rule

📖Requirement Management Life Cycle

Requirement types

❶**Business Requirements** enterprise goals, objectives, needs (why a project is initiated, what will achieve metrics to measure success) ❷**User Requirements** statements of stakeholder needs, how stakeholder will interact with a solution, bridge <Business Requirements> to other requirements classes ❸**Functional Requirements** behavior/ information/ capabilities to perform ❹**Quality of Service Requirements** (non-functional, supplementary requirements) ❺**Assumptions/ constraints** aspects of problem domain limiting/ impacting design but not functional requirements ❻**Implementation requirements** to transition from current to desired future state (once off) ❼**Project requirements** ❽**Quality requirements**

Elicitation Importance

❶**Support executive decision making** ❷**Apply influence to finish work** (backed by information that supports the goals) ❸**Assist in negotiation/ mediation** ❹**Resolve conflicts** ❺**Define real problems**

Requirements Elicitation

❶Brainstorming ❷Document analysis ❸Focus group ❹Interface analysis ❺Observation ❻Prototyping ❼Requirements workshop ❽Reverse Engineering ❾Survey/Questionnaire

Requirements Communication

❶Requirements communication plan ❷Requirements format ❸Requirements package ❹Requirements presentation ❺Conduct a formal requirements review ❻Get signoff

Requirements planning and management

PLANNING •key planning impact areas •SDLC •project life cycle methodology •project risk, expectations & standards •key stakeholder needs & location •project type REQUIREMENTS ACTIVITIES •requirements elicitation stakeholders/ activities •requirements analysis/ documentation activities •requirements communication activities •requirements implementation activities ESTIMATE REQUIREMENTS ACTIVITIES •milestones in requirements activities development/ delivery •units of work •effort per unit of work •duration per unit of work •identify assumptions •identify risks MANAGE REQUIREMENTS SCOPE •establish baseline •structure for traceability •identify impacts to external systems •identify scope change resulting from requirement change (change management, maintain scope approval) MEASURE/ REPORT ON REQUIREMENTS ACTIVITY •determine project / product metrics •collect project / project metrics MANAGE REQUIREMENTS CHANGE •plan requirements change •understand requirements changes to •document requirements changes •analyze change requests

52 Techniques to analyze process

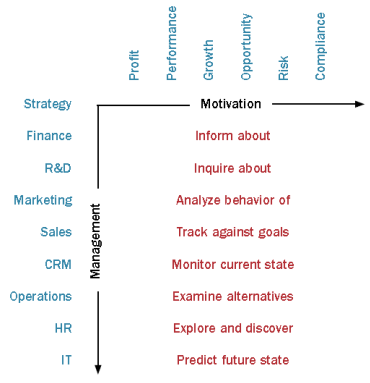


Figure 1. Scope of BI business requirements

1 Who owns process **2** Who has power to change it **3** What are its objectives **4** What are success metrics **5** Who are customers **6** Who participate **7** What are inputs **8** What analytical tools **9** What events and milestones drive this process **10** What kind of decisions does this process generate **11** What decision-making criteria **12** How are decisions communicated, and to whom **13** Link to other management systems

53 Risk Management

❶Identify ❷Analyze ❸Plan ❹Implement ❺Track & Control

Step 1 – Identify

1-1 Identify and Collect **Candidate Risks** **1-2** Identify & Provide Candidate Risk Input to Risk Manager/Analyst **1-3** Review Candidate Risks (**Table 1:** Criteria for Risk Identification - Risk? Impact? Likelihood? **Table 2:** *Risk Identification Components* – Originator, date, title, description, context) **1-4** Record Identified Risks in the Project Risk Database

Step 2 – Analyze

2-1 Verify/Determine **8 Risk Classification** ❶Cost ❷Schedule ❸Scope ❹Quality ❺Human Resources ❻Communications ❼Procurement ❽Integration

2-2 Verify/Determine **Risk Impact** (*High, Medium, Low*) **2-3** Verify/Determine **Risk Probability** (High >65% conf., Medium 35-65%, Low <35%) **2-4** Verify/Determine **Risk Timeframe** (*Short <120 days, Medium <360 days, Low*) **Risk Exposure** = Probability x Impact **2-6** Verify/Determine **Risk Severity** = *Exposure x Time Frame* **2-7** Recommended **Mitigations + Contingencies**: *Elimination, Reduction, Acceptance* **2-8** Review Risks with Project Director, Project Sponsors, and Stakeholders

Step 3 – Plan

3-1 Assign **Risk Owner** **3-2** Develop-Review-Approve Mitigations, Contingencies, Measurements **3-3** Develop Mitigation and **Contingency Action Plans** **3-4** Update Project Risk Database

Step 4 – Implement

4-1 Execute Mitigation and Contingency Action Plans **4-2** Update Project Risk Database

Step 5 – Track and Control

5-1 Oversee Mitigation and Contingency Action Plan Execution **5-2** Track Action Plan Execution and Provide Feedback **5-3** Re-Assess Risks **5-4** Report Risk Status **5-5** Maintain the Project Risk Database **5-6** Escalation of Project Risk **5-7** Risk Retirement

Table 8: Guide for Determination of Risk Escalation

Risk Escalation	Risk Severity			
		High	Medium	Low
Project Criticality	High	CHHSA	CHHSA	Sponsor/OSI
	Medium	CHHSA	CHHSA	Sponsor/OSI
	Low	CHHSA	Sponsor/OSI	Sponsor/OSI

See PMI Practice Standard Risk Management

Risk Statement "Because of <1 or more causes>, <risk> may occur, which would lead to <1 or more effects>

PM Risk TOOLS

Identify ❶Brainstorm ❸Constraint analysis ❷Cause & Effect (Ishikawa) ❸DELPHI ❹FMEA Failure Modes Effect Analysis ❺Force Field ❻Influence diagram ❼Risk breakdown structure ❽Questionnaire ❾WBS review ❿SWOT

Analyze ❶Probability and Impact ❷Post-review ❸Analytic Hierarchy ❹Root-Cause ❺Decision Tree ❻Expected Monetary Value EMV ❼Monte Carlo

Plan ❶Brainstorm ❷Contingency planning ❸Contingency Reserve Estimation ❹Critical Chain Project Management CCPM ❺Prompt List ❻Scenario Analysis

Track & Control ❶ Critical Chain Project Management CCPM ❷Reserve Analysis ❸Risk Audit ❹Trend Analysis ❺Variance Analysis

Risk Register ❶**SUMMARY** ◆Risk statement ◆Risk owner ◆Date last assessment ◆Due date for update of risk assessment ◆Risk category (Strategic, Project delivery, Operational) ◆Risk classification (low, medium, high) ◆Risk response ❷**DESCRIPTION** ◆Title ◆Scenario description (Actor, Threat type, Event, Asset/resource, Timing) ❸**ANALYSIS RESULTS** ◆Frequency of scenario (# times per year) ◆Impact on business (1 Productivity 2 Cost of response 3 Competitive advantage 4 Legal) ◆Impact rating (average of 4 impact ratings) ◆Rating of risk (frequency & impact ratings) ❹**RISK RESPONSE** ◆Response (avoid, mitigate, transfer, accept) ◆Response Justification ◆Risk action plan status, issues ◆Completed responses status, issues ❺**RISK INDICATORS**

📖**CRISC IT Risk & Controls** **5 practice areas** ❶Risk Identification, Assessment, Evaluation ❷Risk Response ❸Risk Monitoring ❹IS Control Design & Implementation ❺IS Control Monitoring & Maintenance 📖**IT Risk Scenario 5 Components** ❶Actor ❷Threat type ❸Event ❹Asset/Resource ❺Time 📖**Risk Analysis and Response** **Risk Analysis** Top Down/ Bottom Up **5 Risk Factors** ❶External environment ❷Internal environment ❸Risk management capability ❹IT capability ❺IT-related Business Capability **4 Risk Response** ❶Avoid ❷Mitigate ❸Transfer ❹Accept **Risk response 5 parameters** ❶Cost ❷Importance ❸Implementation capability ❹Response effectiveness ❺Response efficiency **36 Risk Scenarios** ❶IT program selection ❷New technologies ❸Technology selection ❹IT investment decision making ❺Accountability over IT ❻Integration of IT within business processes ❼State of I/F technology ❽Ageing of application SW ❾Architectural agility & flexibility ❿Regulatory compliance ❶SW implementation ❷IT project termination ❸IT project economics ❹Project delivery ❺Project quality ❻Selection/ performance of 3rd-party ❼IF theft ❽Destruction of IF ❾IT staff ❿IT expertise & skills ❶SW integrity ❷IF HW ❸SW performance ❹System capacity ❺Ageing of IF SW ❻Malware ❼Logical attacks ❽Information media ❾Utilities performance ❿Industrial action ❶Database integrity ❷Logical trespassing ❸Operational IT errors ❹Contractual compliance ❺Environmental ❻Acts of nature

Fighting Resistances to Changes

📖Types of Resistance 📖Risk Management

1 Resistance: Initiative significant change for customers

❶Understand the exact nature of the change for the customers, what they will have to do that is new or different (This refers to CIBC's external customers) ❷Involve Marketing to create a ***communication strategy*** that includes both customers and customer-facing employees ❸Identify customer- facing employee knowledge/skill gaps and get Training involved to develop an action plan.

2 Resistance: Rationale hard to understand & communicate

❶Develop a ***Stakeholder Role Map*** to identify key audiences affected by the initiative ❷Develop a ***cascading communication strategy***, so that difficult to understand messages can be conveyed face-to-face by the one-up manager ❸Develop ***feedback mechanisms*** – Employees Hot Lines, Mailboxes and/or Town Hall Meetings or Workshops designed to convey the messages with time for Q&As

3 Resistance: Employees must change behavior to succeed

❶Develop a ***Stakeholder Role Map*** to identify key stakeholders ❷Identify the nature of the behaviour change – discuss with sponsor/steering committee and get agreement ❸Involve Training to develop a ***strategy/plan to shift behaviour*** ❹Involve HR to determine if/how to incorporate it into ***Performance Scorecards*** ❺Identify incentives that can be introduced ❻Develop a ***cascading communication strategy***. Ensure sustaining sponsors are fully engaged (they know, understand, communicate and are prepared to deliver consequences) ❼Develop a strategy to measure the behaviour change

4 Resistance: Significant knowledge & skill required

❶❷❸❹❺❻❼Above ❽Assess capability against future skill, attribute requirements

5 Resistance: Expected resistance from affected employees

❶Develop a ***Stakeholder Role Map*** to identify the different stakeholder groups who will be impacted by the initiative ❷Upon completion of the ***Resistance Assessments***, develop a strategy and action plans to mitigate and track the level of resistance among the various stakeholder groups.

6 Sponsorship: Accountable managers not support change

❶Develop a ***Stakeholder Role Map*** and identify the critical ***Sustaining Sponsors*** of the key targets of the change ❷Determine whether the Sustaining Sponsors are also targets of the initiative ❸Develop a strategy and action plans to mitigate and track the level of sponsorship among the various Sustaining Sponsors.

7 Sponsorship: Implementation involves many people

❶Develop a ***Stakeholder Role Map*** to identify the different stakeholder groups who will be involved in the initiative. Include all relevant areas e.g. Risk Management, HR, Security, Compliance, Finance etc. as well as outside suppliers, labour unions ❷Determine the nature of their involvement ❸Identify ***critical Sustaining Sponsors*** for each of the areas identified ❹Identify ***critical change agents*** you need to enlist in those areas ❺Develop an ***advocacy strategy*** to gain and track sponsorship in the respective areas so that you can work effectively with required change agents

8 Sponsorship: Sponsors not grasp time, $, HR reqmnts

9 Sponsorship: Sponsors not provide resources

❶Develop a ***Stakeholder Role Map*** and identify the ***critical Sponsor / Sustaining Sponsors*** of the key targets of the change ❷Develop a strategy to communicate critical resource requirements to the Sponsors. The ***Project Charter*** is an effective vehicle to use to discuss these issues ❸Revise the scope of the project to reflect the resource commitment that can be made by the Sponsor/Steering Committee ❹Develop an ***effective working contract*** with the Sponsor/Steering Committee to ensure these issues can continually be addressed through the ***Phase Transfer*** or between as required.

10 Sponsorship: Coordinate various business groups

❶❷❸❹As in 8 ❺Develop an ***advocacy strategy*** to gain and track sponsorship in the respective areas so that you can work effectively with required change agents. (The Initiating Sponsor of the initiative and the Project Steering Committee will need to play an active role in enlisting the co-operation of the various business groups)

Experiences

•**15 yrs** in portfolio management; **$100M portfolio of 100** programs and projects. •**20 yrs** of program/ project management + developing/ deploying project management standards, processes, tools for project delivery and **budget** and **benefits**, **system integration** •Manage/ report scope, time, cost, risk, resources, quality in programs exceeding **$50M** of **$15M** with **10** concurrent projects and teams **120** resources and **20** vendors •Formulated corporate IT strategy for **CIBC**: $80M 3-yr upgrade financial risk system for $2B reduced Regulatory Capital; **CIBC Mellon**: $6M 2-yr integration financial system for revenue of $350M and 1,300 employees; and **AIG** $10B in revenues 120% explosive expansion into China, India, VN •Delivered AIG's **4 strategic objectives** at $70M in costs per objectives, inventory of 9 regional initiatives; prepared business cases and effective ranking, prioritizing, approving and executing projects •Created an inventory of **9** initiatives supporting **4 x $70M** strategic objectives; established rigorous financial procedures for business cases and project ranking, prioritizing, approving and execution •Strategy **for e-services** for 10 Australian industrials combined export of $50M to 20 countries in Asia and Middle East •**Tier-1 consulting** projects for business transformation, process reengineering, compliance, infrastructure, development •**Projects rescue** (Capital Markets, Credit Cards, Retail Loan, ***Wealth***, ***Treasury***, Payment, Business Intelligence, Insurance) and public services (BColumbia Corporate Accounting Services, MTO, Australia HCS)	•Built consensus with senior leaders, management and staff. Team motivation, mobilization, building complex relationships among business lines, internal staff and vendors. Expert in identifying stakeholders expectations, and aligning them optimally •Set up **Project Management Office** at AIG, CIBC (Financial Risk), CIBC Mellon, SIERRA, HOOPP, CBOC •Portfolio management, **Program management** •Within PMO, mentored and managed **15 program and project managers** •Engaged various business units for adoption and maturity of program and project management disciplines •Defined **PMO policies and procedures** with the focus on transparency and alignment with strategic objectives for all programs and projects in the portfolio •Defined **governance processes** around Portfolio and Project Management tools then evaluated, deployed and institutionalized **CA Clarity** and **PLANVIEW** systems •Established policies, procedures, processes, tools & templates for portfolios, programs, and projects Metrics, **estimation**, **Balanced Scorecards**, **Strategy Maps**, **Activity-Based Costing (ABC)** and **Earned Value Management**. Developed project accounting practices and managed Project Financials using Scotia Bank SMARTSTREAM, Project Reporting Facility •Expert with Program, Project Management methodologies including PMI's Standard for Portfolio/ Program/ Project Management; Ontario Public Service Unified Project Management Methodology, Oracle Application Implementation Methodology, others

•Implemented **Governance Methodologies** (Sarbanes-Oxley Act, COSO, COBIT, VallT, CMM, RiskIT, ISO, ITIL); re-designed mgt processes for 5 departments (operations, middle office, back office, finance, IT) 200 members/ staff and established more than 4,000 process controls (SOX) at CIBC **5 business units and 7 stakeholders financial/compliance** standards: IFRS (HOOPP), GAAP (MANULIFE), BASEL II&III (CIBC), SOX (CIBC, AGNICO)	(Scotia, CIBC, AIG, PwC), **AGILE**, **RUP**, **SDLC**, **SIMCORP** •**Project rescue missions** •**project auditing** •scope management •**vendor selection** • **vendor management** (RFQ, RFP, contract negotiation, SLA, performance monitoring) •Project governance •Business requirements •Business process transformations, enterprise risk, change management: assessed current state, defined target state, implemented gaps for org. changes
•Work with clients to define/ **manage scope, strategy, and requirements** of projects •Work with clients to manage **implementation** of projects •Develop **cost benefit** analysis •**Complete** projects within budget/ timelines while meeting client business objectives	•Identify and analyze project **risks** •Mitigate, document, control project **risks** •Develop and deliver **budgets** •Identify **resource** needs for project •Establish **roles, expectations, and goals** for team members •**MS PROJECT**, **SHAREPOINT**, **EXCEL**, **ACCESS**

Action Verbs

Refreshed the **PMO engagement model** - Designed and deployed - Led oversight and execution - Designed new processes - Provided a foundational baseline of - Developed cross-functional change management governance models - Set expectations, facilitated initial knowledge transfer and managed on day to day basis efforts - Managed Mutual Funds Project, resulting in updates to 100% of procedures (**80 existing procedures, 130 new procedures**), and in updates to more than **40 mutual fund products**- Defined I&IT **Project Portfolio**; Defined I&IT **Portfolio and Project Management policy**; Established I&IT **PMO strategy, guiding principles, functions, org structure, staffing and career paths, Checkpoint and Gating guidelines**, Established resource management process and supporting tools, Created a set of **43 Project Management artifacts**, including **process maps, document templates**, guidelines and process guides for **Initiation, Planning, Execution and Closeout** phases defined in the methodology. The artifacts covered Project Management (**Project Tailoring Guidelines, Project Charter, Project Schedule, Project WBS, Project Management Plan, Project Estimation Guidelines, standardized rates**, others), **Business Analysis, Solution Architecture, Quality Management** and other areas; Facilitated implementation of the **Project Intake Process** to standardize assessment / ranking of 6 new project and program requests per month

INTERVIEW QUESTIONS

INTERVIEW QUESTIONS TO ANTICIPATE:

What interests you most about the company?
What interests you most about the job description?
Describe yourself.
Describe yourself in 2-3 words.
Why do you feel you would be the best candidate for this position?
What are your strengths/weaknesses?
What would your current boss say your strengths are?
What changes have you made to make yourself more effective at work?
What areas do you feel training would be beneficial?
Describe a difficult situation at work and how you handled it.
What motivates you?
Give me an example of a time you procrastinated and how you handled it.
Give me 2-3 process improvements you identified and implemented.
How do you set priorities?
Describe your most successful manager.
If you could start your career all over again, what would you do differently?

INTERVIEW QUESTIONS TO ASK:

What have you enjoyed most while working at XYZ company?
What have been your largest accomplishments at XYZ company?
How has turnover been within the company?
How much growth within the department and company have you seen since you have been on board?
Do you think the departments collaborate well within the organization?
Does the company typically promote from within?
What is the accounting department like?
What are the most important attributes for the person to succeed in the position?
What skills are currently missing on the team that you look for in a new hire?
What are the most important projects for this position over the next few months?
What are the biggest areas for growth within the company within the next year?
What are the biggest challenges for the company and accounting department?
Anything that concerns you about my background being a good fit for this role?

GENERAL

1. Tell me about a time where you had to manage change. How did you do it, and what was the outcome?
2. How would you describe your management style?
3. How would you describe your ability to communicate with senior management?
4. What qualities make a good boss or manager?
5. What are your greatest attributes as an employee?
6. What are your career goals?
7. In your last performance evaluation, where were your areas for improvement?
8. Why did you leave your previous employer, or why are you leaving your present job?
9. Where do you hope to be in five years?
10. Which of your past jobs was the most interesting?
11. Which of your past jobs was the least interesting?

BEHAVIORAL

12. Describe a recent situation in which you imparted your key points to a group with varying verbal skills?
13. Describe a time when you communicated something unpleasant or difficult to say to your manager. How did you assert yourself?
14. Give me an example of a time when you confronted a negative attitude successfully, which then resulted in building teamwork and morale.
15. Tell me when you had to "stand up" for a decision you made even though it made you unpopular.
16. Tell me about a time when you showed high enthusiasm and energy in order to create a positive energy in others. Give a specific example.
17. What is your viewpoint about co-workers that never speak their mind?
18. What sources of information have provided you with the best data for decision making?

PERFORMANCE-BASED

19. What are you looking for in a new job?
20. Why is having "x" and "y" important to you, and why do you think that this job meets that criterion?
21. Tell me about your schooling and advanced training.
22. What is your major project or accomplishment ?
23. Tell me about a major team accomplishment; consider one where you led a team and one when you were a key member of a team.
24. One major problem we are now facing is "xyz". How would you go about addressing this? a. What would you need to know, and how would you plan it out? b. What have done that is most similar to this?
25. While I've seen a few other strong candidates, I'm impressed with some of the work you've done. What are your thoughts now about this job? Is this something that you'd consider further? Why or why not?

FACT FINDING

26. Describe a significant work challenge that you've had to overcome. Why was it significant?
27. What were the actual results?
28. When did this take place and at what company?
29. How long did it take you to complete the task?
30. What was the situation when you took on the project?
31. Why were you chosen for this role? Did you volunteer?
32. What was your actual title?
33. Who were the people on the team?
34. What was your supervisor's title?
35. What technical skills were needed for the task?
36. What skills were learned? Describe the planning process, your role in it, and whether the plan was met. Provide details of what went wrong and how you overcame them. What was your role in this project?
37. Give me 3 examples of where you took the initiative?
38. What were the biggest changes or improvements?
39. What was the toughest decision you had to make? How did you make it? Was it the right decision? Would you make it differently looking back?
40. Describe the environment – the pace, the resources available, your boss, the level of professionalism.
41. What was the biggest conflict you faced? Who was it with and how did you resolve it?
42. Give me some examples of helping or coaching others.
43. Give me some examples of where you really had to influence or persuade others to change their opinion.
44. How did you personally grow as a result of this effort?
45. What did you like the most and least?
46. In retrospect, what would you do differently?
47. What type of recognition did you receive for this project? Was it appropriate in your mind?

INTERPERSONAL SKILL

1. **Emotional Self-Awareness** – the ability to recognize and understand one's feelings and emotions, differentiate between them and know what caused them and why.
•Benefit in the Workplace? Good emotional self-awareness promotes conflict resolution and leads to improved interaction between staff. Is it easy for you to know when you are getting anxious, scared, annoyed, or angry? Can you give me an example or explain to me how you know this? What things do you feel really happy about? Why? What things do you feel really sad about? Why?

2. Assertiveness – ability to express feelings, beliefs and thoughts and defend one's rights in non-destructive manner.
•Benefit in the Workplace? Proper assertiveness helps individuals to work more cohesively and to share ideas effectively. When you disagree with someone, what do you typically do? Give me an example of when you did that? Do you have difficulty standing up for your rights?

Give me an example of when you did. When someone's behavior consistently bothers you, how do you usually react? Can you give me an example of when you dealt with this situation and how you handled it?

3. Self-Regard – To respect and accept oneself as good.

•Benefit in the Workplace? Employees who have a high self-regard have better work attitudes and behaviors. Better self-confidence means better performance. What are your strengths, and how do you use them to your advantage? Can you give me an example? What are your weaknesses and what are you doing to improve them? Can you give me an example? Describe what kind of person others would say you are. Why?

INSIGHT INTO BEHAVIORAL-BASED QUESTIONS

4. **Self-Actualization** – To realize potential capabilities and to strive to do that which one wants to do and enjoys doing.

•Benefit in the Workplace? High self-actualization is connected with good motivation + team performance. What are your short-term goals and long-term goals? What are you doing to accomplish these goals? How actualized do you feel you are? Why? What things interest you and why?

5. **Independence** – The ability to be self-reliant and self-directed in one's thinking and actions and to be free of emotional dependency.

•Benefit in the Workplace? Independence increases productivity and efficiency in work flow and the ability to meet milestones + goals in a timely manner. How do you make difficult decisions? Give me an example of a difficult decision that you had to make and the process you used for making it? Do you need people more than they need you, or the opposite? Why? What interest you and why?

6. **Empathy** – the ability to be aware of, to understand, and to appreciate the feelings of others. It is "tuning in" to what, how and why people feel the way they do.

•Benefit in the Workplace? This creates a more cohesive, functioning team and better team players. How difficult or easy is it for you to understand how people feel? Do you usually know when you have said or done something that has offended someone? How do you know? What do you do about it? Can you give me an example of a time when you felt you might have offended someone? What did you do?

7. **Interpersonal Relationships** – to establish and maintain mutually satisfying relationships that are characterized by intimacy and by giving and receiving kind gestures.

•Benefit in the Workplace? Good interpersonal relations translate into effective communication within and between departments and groups. When you are in a social situation with people you don't know, what do you typically do? What is the basis for a good relationship in your opinion? What are the ingredients that go into it? Tell me about a relationship that is meaningful to you and what do you do to try and maintain it?

8. **Social Responsibility** – To demonstrate oneself as a cooperative, contributing, and constructive member of one's social group. This involves acting in a responsible manner although one may not benefit personally.

•Benefit in the Workplace? Social responsibility means recognizing departmental and company goals and contributing to these goals. Can you give me an example of a situation where you considered the needs of others, possible to your own detriment? Give me an example of how you behave as a team member?

ADAPTABILITY SKILLS

9. **Problem Solving** – to identify & define problems as well as to generate and implement potentially effective solutions.

•Benefit in the Workplace? The method used for problem solving is critical: viable alternative solutions must be considered, including cost / benefit analysis and long term implications, as examples. Can you give me a step-by-step example of a difficult situation that you handled at work or at home? Is it generally easy or difficult for you to come up with a number of possibilities for approaching a problem? How easy or difficult is it for you to decide on the best solution and implement it? Can you give me an example?

10. **Reality Testing** – the ability to assess the correspondence between what is experienced (the subjective) and what in the reality exists (the objective).

•Benefit in the Workplace? It is important to focus on practicality and not on unrealistic expectations. Do you usually assume things and jump to conclusions, or do you check things out before acting? Can you give me an example? Would others say you are realistic or idealistic and why? Can you give me an example of that?

11. **Flexibility** – to adjust one's emotions, thoughts and behavior to changing situations and conditions.

•Benefit in the Workplace? Employees perform better in positions where tasks are dynamic and changing. Low flexibility resources perform better in more well-defined tasks requiring reliability and consistency. Can you give me an example of when your opinion about a person or situation was clearly wrong and what you did? Give me an example of how well you deal with change in general? If you were forced to leave your home, how would handle it?

STRESS MANAGEMENT SKILLS

12. **Stress Tolerance** – the ability to withstand adverse events and stressful situations without "falling apart" by actively and positively coping with stress; the ability to weather difficult situations without getting too overwhelmed.

•Benefit in the Workplace? Effective stress tolerance has to do with managing reasonable workloads, establishing clear priorities and meeting realistic deadlines. What tactics do you use to cope with everyday stress? Give me an example of a stressful situation that you coped with effectively?

13. **Impulse Control** – the ability to resist or delay an impulse, drive, or temptation to act. It entails the capacity for accepting one's aggressive impulses, being composed, and controlling aggression, hostility and irresponsible behavior.

•Benefit in the Workplace? Rash actions can be costly. Mistakes can often be avoided simply taking the time to stop and think things through. Can you give me an example of a situation in which you were very angry and what you did in that situation? How do you typically deal with an impulse or temptation to act prematurely?

GENERAL MOOD

14. **Happiness** – the ability to feel satisfied with one's life, to enjoy oneself and others and to have fun.

• Benefit in the Workplace? Positive moods lift spirits, create resonance and help overall performance of individuals and teams. If I were to ask your friends how you make them feel when they are around you, what would they say? Why? Are you generally satisfied with the way things are presently going in your life? Why?

15. **Optimism** – to look at the bright side of life and to maintain a positive attitude, even in the face of adversity.

•Benefit in the Workplace? An optimistic attitude helps ward off stress while creating resonance that increases one's productivity. How do you typically deal with failure? Can you give me an example of a time where, in your opinion, you failed? How did you deal with the situation? How do you cope with your pessimistic feelings?

NASA Shared Voyage

•Projects usually present a bundled set of challenges demanding that people operate in both known and new domains at the same time. The known domains are amenable to technical expertise and managerial authority. The new challenges - ***adaptive challenges*** **-** require leadership that can handle the conflict and messiness of ongoing structural tensions across different organizations and groups as they strive for collective innovation.

❶Adaptive leadership is active and reflective: constantly alternate between participating and observing; be part of the action and yet also rise above it to analyze more clearly changing landscapes requiring ongoing corrective action; be able to "get off the dance floor and get on the balcony." **•Adaptive processes in evolutionary biology are experimental**. Rather than investing the knowledge in high authority, which makes sense for technical problems, adaptation is more likely to succeed with a distributed intelligence.

❷Adaptive work generates tough trade-offs between legitimately competing claims, "the difference between 'desirements' and requirements." •Discovering which trade-offs to make requires drawing out divergent perspectives, orchestrating conflicting views and interests, and listening for the crystallization of a good idea rather than reaching too quickly for decision. •But trade-offs are painful. Jobs are lost, people are let go. Casualties are often necessary. Have the stomach to deliver bad news, and the heart to deliver it well.

❸Leadership is a political activity, even in projects. When people make the classic leadership error of treating adaptive challenges like technical problems, they end up assuming too much about the relevant stakeholders and then step on toes unwittingly. Everybody has a piece of the turf, and you'd best respect that. You never know how much your lack of respect may cost you.

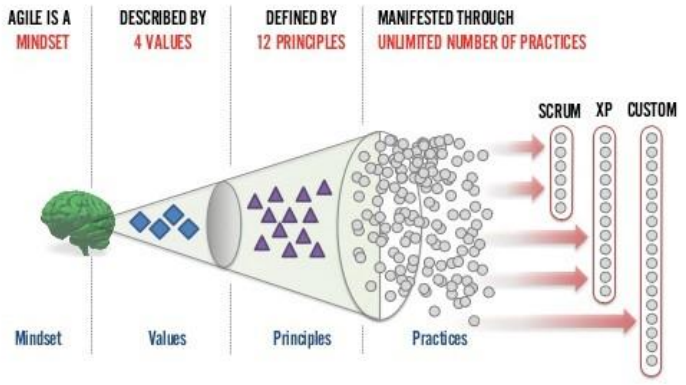
❹Leadership is about challenging people to take far-reaching responsibility**.** The task is to put the creative work back in people's laps when parochial views inhibit new thinking and necessary collaboration. "I don't know how you're going to figure this out, but I have confidence that you will, and if you don't, we all fail."

❺Adaptive work takes time. Within days, we can complete the analysis that was the technical part of the problem-solving. The implementation, on the other hand, took months because implementation consists of changing people's hearts, minds, and habits of behavior. People will either sustain the direct loss of their own job, the indirect loss associated with a friend or colleague losing their job, or the loss of competence for a period of time during which they must learn new competencies. Closer to where the tire hits the road, implementation is more than execution, it demands of people that they face some losses and learn new ways.

❺Leadership infuses the work with meaning. People are willing to take risks, and even pay dearly, if the stakes are sufficiently meaningful. Money is only part of it

MICROSOFT AGILE (FORBES)

	The Agile mindset	The bureaucratic mindset
Goal	The *Law of the Customer*—an obsession with delivering steadily more value to customers.	*The Law of the Shareholder*: A primary focus on the goal of making money for the firm and maximizing shareholder value.
How work gets done	The *Law of the Small Team*—a presumption that all work be carried out by small self-organizing teams, working in short cycles, and focused on delivering value to customers	*The Law of Bureaucrat*: A presumption that individuals report to bosses, who define the roles and rules of work and performance criteria.
Organizational Structure	The *Law of the Network*—the presumption that firm operates as an interacting network of teams,	*The Law of Hierarchy*: the presumption that that the organization operates as a top-down hierarchy, with multiple layers and divisions.



❶Pursue "Agile at Scale," not "Scaling Agile"

Tight focus on delivering continuous value to customers, not merely generating quarterly profits or boosting the current stock price. It also rests on a deep respect for the talents and capacities of those doing the work, and the teams in which they work, not treating workers as "resources" that are assignable, optimizable and ultimately disposable.

❷Take Care of Planning and Coordination

Planning begins with an overall vision for the product. Then a program manager like Aaron develops and owns what is called a "scenario," which is the goal for the product for the next 18 months. It's a story of where the program wants to be 18 months from now. The story can include other teams. The group has about a 60% confidence in its ability to predict what the customers want to and to deliver that. The year is broken up into two seasons, called "spring" and "fall". At all times, each team maintains and owns a thoughtful and detailed three-sprint plan, each sprint comprising three weeks. The team always has a good idea what's in store for the next three sprints.

❸Get the Right Balance of Alignment and Autonomy

Alignment at the top and autonomy at the bottom. The teams need autonomy. That's what drives them to come to work and deliver great stuff. But at the same time, their work has to be aligned with the business.

❹Master The New Role of the Manager

What happens when a team misses a sprint? A manager doesn't monitor a teams' burn-down charts. The burn-down charts are for the teams. If they get behind, guess what they do? They talk about what to do. That's the behavior the manager wants

❺Handle Dependencies At The Team Level

Every three months, there's a standing meeting across all of the teams. It's called "a feature team chat." Every team comes in and shares their plan.

❻Ensure Continuous Integration

Continuous delivery has meant more modularity in design and a change in architecture. The teams use what they call "feature flags." Here's a high level description of how it works. If they are going to do something new, the very first thing that they do is to isolate the code that they are changing and build a switch into the code. It is powered by a flag in the database. It's a configuration change. When the team writes code, they write it behind the safety of the flag. At some point, when they feel it's ready, they can turn it on just for the team. That switch is not a global switch. It's a switch for an account in the system just for the team. If that goes well, then the team can turn it on for certain customers. Those customers can see it and try it. They help the team find bugs and problems. When the team gets through all that, and the team thinks it's really ready, they prepare the release notes and an announcement that they are going to flip the switch for everybody. Then they go back and refactor the old code out. This enables the teams to work alongside each other on the same code without breaking one another's work. At the end of every sprint, the team sends out an email to all 450 people in the Visual Studio Online group and the leadership team. They talk about what they accomplished that sprint and what their plan is for the next sprint. And they record a 3-5 minute video. (Warning: the videos can get fancy, if the teams have aspiring Hollywood directors.) The video replaces the sprint demo.

❼Keep On Top Of Technical Debt

"Now the bugs never grow. There 's a Key Performance Indicator (KPI) we call 'the bug cap.' It's the number of engineers on your team times four. So if you have ten engineers, your bug cap is 40. If you get to 40 bugs, the team needs to stop work on new features and the next sprint, get the bug count back down below 40. It's self-managing.

❽Embrace DevOps and Continuous Delivery

Development and operations merge. The teams own the planning of each new feature. They own the execution of the feature. They own the delivery the feature. And they own the operation of the feature. The change in time frame makes a big difference. A deadline now is three weeks. Three weeks is no big deal. Before you had only two opportunities., and if you missed it, you had to wait two years. Now if it's not high quality, you don't push it out. You hold it. It's disappointing that you didn't get it out. You talk about it in your retrospective. Did you do something wrong? Or did you just underestimate the level of complexity? Did you miss something? It's better to have that conversation than to have a fire-drill and punish the team for not delivering what they promised, or worse, pushing out a poor-quality product.

❾Continuously Monitor Progress

The teams do a great deal of monitoring how the features are being used. The results flow into the aspirational backlogs, which are called scenarios. Every month, the program manager reports out on metrics, on the accounts using different aspects of the service. So the group is learning to become a data-informed business. They don't call it "data driven" because that would run the risk of missing the big picture. They use their brain and their gut feel as well as being informed by the data. The data isn't an after-thought though. It's often the first part of the conversation. Part of the very definition of "done" is having the right telemetry. The teams see this data and monitor it both when they are testing it and as soon as it goes live. It's not something they do in the sprint after they ship it. It's part of the acceptance criteria to ship.

❿Listen To Customer Wants, But Meet Their Needs

The teams don't blindly follow what customers say. They have what they call "the cookie principle." If you have a plate of cookies and you ask people if they want one, they will say yes. No one turns down a cookie.

❶Deal With Directions from Above

There is very little load balancing among teams. If a team gets behind, they don't break up the team or move individuals to the team to fix it. They ask the team itself to fix the problem. They try to keep the teams together for 12 or 18 months. That's what the teams themselves like. The firm is making an investment in the team for at least nine months or a year.

❷Use Self-forming Teams To Encourage Team Ownership

Managers let people choose which team to work on. People can reshuffle every 18-24 months. Around two thirds of the team members decide to stay where they are. As a result, there are not many brand new teams. But the team members have the choice. The result is a significant investment in persistent teams. Quite apart from team well-being, it leads to higher performance. The team owns the backlog. Of course, there is a lot of discussion about priorities. But a manager doesn't tell the team what should be next on the Kanban board.

❸Recognize that The Team is the Product

Microsoft has an advantage: it had teams, long before they went Agile. There was already a strong team culture. It's more difficult for firms going Agile that don't have a history of teams.

❹Build Quality From The Beginning

In the first sprints, there was agreement on 3 week sprints. The leadership signed off on the idea of Agile and Scrum, but they were a little worried as to how it was going to work. So they planned for "a stabilization sprint" after five sprints. The goal is to avoid the sequence: write code in the first sprint. Test it in the second sprint. Fix bugs in the third sprint. The rules of the road are: deliver finished product every sprint.

❺Use Coaching Carefully

External coaches and trainers at Microsoft were noticeable in the site visit by their absence.

❻Ensure Top Level Support

To achieve Agile at scale, the support of corporate vice-president, Brian Harry, has been central. Aaron has had the benefit of living in the Developer Division where Scrum and Agile practices now have a deep foothold. The Visual Studio group is leading the charge for Microsoft as a whole. It owns the "first party engineering system charter" (IES) and is driving that across the company. There are monthly scorecards on how the big divisions are doing in adopting it.

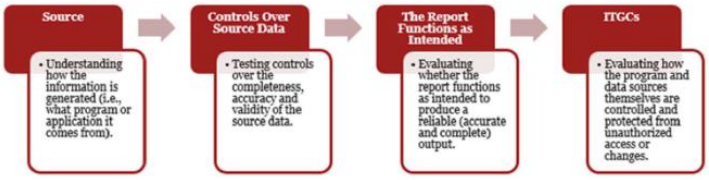
AIG AUDIT

FCU

◆**ELC** (Entity Level Control) ◆**OSP** (Outside Service Providers) Oversight ◆**LU**= Least (privileged) User Access ◆**NTE**= nature, timing and extent ◆**SSAE16 SOC1, SOC2** ◆**Audit Writing 5C's**: Criteria (what should be), Condition (the current state), Cause (the reason for the difference), Consequence (effect), Corrective action plans/recommendations.

PWC

Key Reports



Accuracy & Completeness Procedures

Report Type	Procedures
Standard ("canned") report	• Validate that the report is standard and no changes were made to the report since system implementation/standard vendor upgrade or patch • Test ITGCs supporting continued reliability of the report • If input parameters are used, verify the input parameters for each report supporting control testing.
Customized Report/Query (subject to ITGCs)	• Test completeness and accuracy of the report • Test ITGCs supporting continued reliability of the report • If input parameters are used, verify the input parameters for each report supporting control testing.
Customized Report/Query (not subject to ITGCs)	• Test completeness and accuracy of each report supporting control testing, including parameters used to generate the report.

Full/False Accept/Reject Testing

• To assess whether the data included in the report is accurate, select a sample of items from the report and agree key attributes within the report to the underlying system.
• To assess whether the data in the report is complete, select a sample of items (different to the one used to test accuracy) from the system and confirm that those items are included in the report using unique key attributes.

Using a data extract, reperform the report/query

• Obtain an understanding of the logic used to generate the report.
• Observe the extraction of the data and confirm that the extraction is complete and apply the logic obtained
• Compare the result to the contents of the report used in management's control to replicate the output by running independent queries on the extracted data on the back end database and match to the output on the report.

Perform an independent code review

• Assess the technical report logic to determine whether the report is generated as intended (i.e. combination or exclusions)
• Utilize sufficient technical ability and knowledge to formulate an independent point of view on the sufficiency of the code to satisfy the intended purpose, including both simple query languages (i.e. SQL) and complex mainframe programming languages (i.e. COBOL)
• Even code written in a simple query language may be complex, affecting the ability to efficiently perform a code review

System Interfaces

Interfaces Considerations

• What are the ways in which data flows from source system to target system, including pass through systems?
• What is the type of data being sent over the interface, and any specific key attributes? Is the data being modified (e.g. filtered, excluded, aggregated) during the transmission?
• How often is the job executed/its frequency for the purposes of the control?
• Where is the job configuration held, either in the source or destination application, or in a job scheduler like AutoSys? Is it subject to relevant ITGCs?

Interface – Interface Job Testing

• Identify the interface job and obtain job details and configurations
• Identify and test controls for handling job abends for the job
• Perform procedures over continued operation of the interface during the period

Interfaces – Testing Completeness

• Extract from source application of the file(s) being sent to destination application, including completeness considerations (e.g. script review and analysis)
• Extract from the destination application of the file(s) received from source application, including completeness considerations (e.g. script review and analysis)
• Reperform the interface by comparing the source file (e.g. total entries, total balance) to the file received in the destination application

Interfaces – Testing Accuracy

For a sample line item(s) selected from the destination extract:
• Obtain transaction details/key fields in the destination system
• Compare those key fields to the transaction details in the source system for accuracy

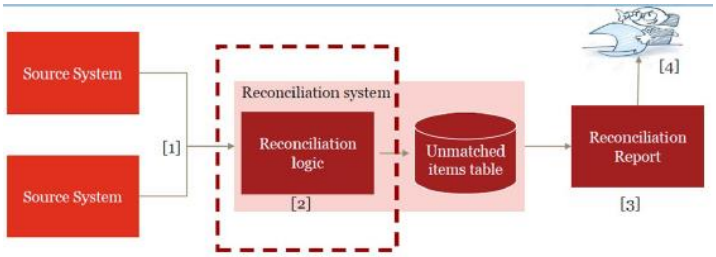
Automated Controls Considerations

• What are the various iterations in which the control can be configured and which ones are in use (e.g. calculation methods, validation checks, etc.)?
• What is the process for periodic validation of the system functionality?
• How and who can overwrite system functionality? And what is the process for implementing the changes?

Testing Automated Controls

• Gain an understanding and evaluate the underlying logic/functionality
• Perform a walkthrough of transactions to demonstrate the operation of the functionality is consistent with business purpose.
• Perform positive and negative scenario testing for each functionality
• Perform testing over each iteration of the functionality

Testing Automated Reconciliations



Reconciliations Considerations

• How the reconciliation is performed (automated vs manual)?
• What is being reconciled (i.e. cash, positions, balances, etc.)?
• What are the key fields being matched?
• Is the source data, including filtering criteria and exclusions, appropriate?
• How many iterations on the matching logic exist?
• What is defined as a break (tolerances/thresholds)?
• How are the results of reconciliation displayed (i.e. exception only, etc.)?
• What is the process for aging & resolution of the reconciling items?
• What is the monitoring over aged items?

Testing Automated Reconciliations

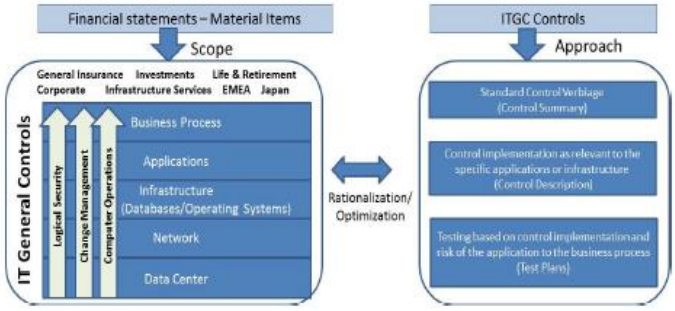
Method 1: Using source data/inputs

• Define Expectation: Obtain source data/inputs & apply necessary filters/exclusions based on systematic logic
• Define Outcome: Obtain results of reconciliation performed by the system (report, dashboard, etc.)
• Reperform Reconciliation: Compare the expectation from #1 vs outcome from #2
Testing Automated Reconciliations

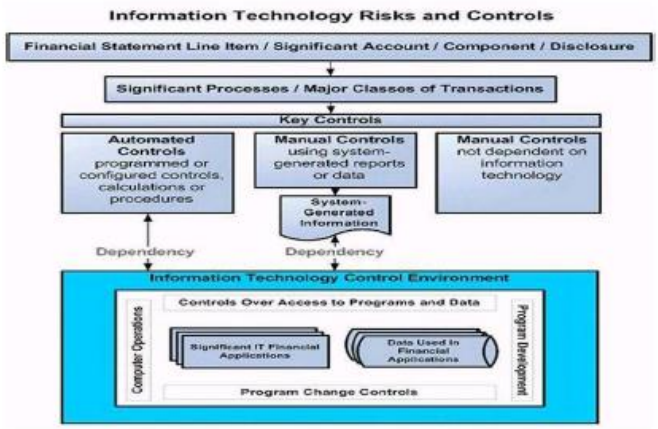
Method 2: System Validation

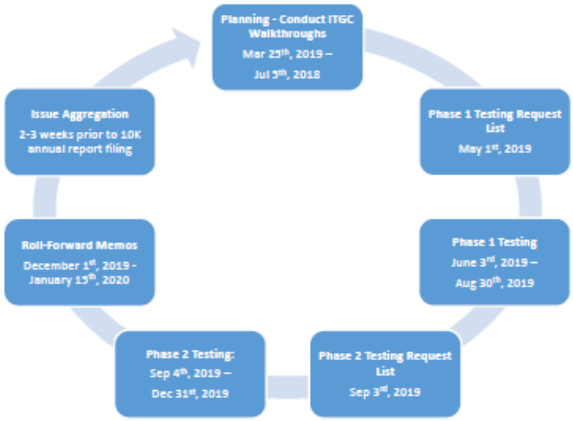
1. Perform walkthrough to gain an understanding of the systems, feeds, and logic associated with the reconciliation
2. Define Expectation - Obtain Positive iterations and Negative iteration (data that matches/ does not match) and submit it into the application/reconciliation tool for processing
3. Define Outcome - Obtain results of reconciliation performed by system for both Positive iterations (which do not create reconciling items) and Negative iterations (which do create reconciling items)
4. Reperform Reconciliation - Compare results of expectation in #2 vs outcome in #3
5. Generation of Key Report - Test that reconciliation results appears completely and accurately Note: consider the effectiveness of ITGCS & test the continued operation of the control throughout the period

Inshoring SOX functions



IT Dependent Controls





RPA

◆Initiated from Accounts Payable (NJ), DBA <Tax, FIS Billing, FP&A Planning&Analysis, Comptrollers> ◆Consultant: GENPACT ◆Process 1: Batch creation + Monies moving ◆Process 2: VOID/STOP Payment (Reversal) ◆Systems AWD (Automated Work Distributor Imaging & Workflow), OASYS PrC (Fixed annuity Admin) ◆ RPA: OPENSPAN PEGASYSTEMS

SOX Controls

NON-CLEARWATER; CLEARWATER

SOC for Service Organizations

SOC for Service Organizations reports are designed to help service organizations that provide services to other entities, build trust and confidence in the service performed and controls related to the services through a report by an independent CPA.

SOC 1 ICFR

Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting - These reports, prepared in accordance with AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting,* are specifically intended to meet the needs of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user auditors), in evaluating the effect of the controls at the service organization on the user entities' financial statements. Two types of reports:

- Type 2 - report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.
- Type 1 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

Use of these reports is restricted to the management of the service organization, user entities, and user auditors.

SOC 2 Trust Services Criteria

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy - These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. Roles:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

Similar to a SOC 1 report, there are two types of reports: A type 2 report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and a type 1 report on management's description of a service organization's system and the suitability of the design of controls. Use are restricted.

SOC 3 Trust Services Criteria for General Use Report

These reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. Because they are general use reports, SOC 3 reports can be freely distributed.

Key Question	Response	SOC Report Type Required
Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC 1® Report
Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organization's systems?	Yes	SOC 2® or SOC 3® Report
Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?	Yes	SOC 2® Report

AICPA Toolkit for SOC for Service Organizations

To help service organizations better understand SOC for service organizations examination engaagements and educate current and potential customers on the reports on their controls, the AICPA has developed the SOC Toolkit for Service Organizations. All materials are available as free downloads. The AICPA has developed the "Information for Management of a Service Organization" document to assist management of a service organization in preparing its description of the service organization's system, which serves as the basis for a SOC 2®examination engagement. It is also intended to familiarize management with its responsibilities when it engages a service auditor to perform a SOC 2® engagement. This document was adapted from the AICPA Guide, *SOC 2® Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (January 1, 2018)*.

AUDIT SKILLS

IIA standards

Standard 1210 – Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

Standard 2010 – Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

2010.A1 – The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

2010.A2 – The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

2010.C1 – The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

Standard 2030 – Resource Management

The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Standard 2100 – Nature of Work

The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

Standard 2110 – Governance

The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

- Making strategic and operational decisions.
- Overseeing risk management and control.
- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

2110.A2 – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

Standard 2130 – Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

Standard 2200 – Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must

consider the organization's strategies, objectives, and risks relevant to the engagement.

Standard 2201 – Planning Considerations

In planning the engagement, internal auditors must consider:

- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

2201.C1 – Internal auditors must establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant engagements, this understanding must be documented.

Standard 2210 – Engagement Objectives

Objectives must be established for each engagement.
2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.
2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.
2210.C1 – Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client.
2210.C2 – Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.

Standard 2220 – Engagement Scope

The established scope must be sufficient to achieve the objectives of the engagement.
2220.A1 – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.

Standard 2230 – Engagement Resource Allocation

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

Standard 2240 – Engagement Work Program

Internal auditors must develop and document work programs that achieve the engagement objectives.

Standard 2310 – Identifying Information

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement objectives.

Audit Metrics

Frequency

Frequency	Responses
Monthly	4
Quarterly	14
Semi-annually	0
Annually	11
Other (please explain)	4

Environment

Performance Measure	Responses
Number of management requests	7
Number of meetings with the organization	2
Number of meetings with executive management	4
Management satisfaction survey results	19
Others (please list with benchmarks as applicable)	6

Output

Performance Measure	Responses
Percent of audit plan completed	25
Number of audits completed	20
Number of advisory services completed	11
Number of recommendations made	8
Number of recommendations implemented	13
Others (please list with benchmarks as applicable)	9

Quality

Performance Measure	Responses
Last external peer review score	15
Auditee satisfaction survey	17
Staff audit experience	10
Number of professional certifications	12
Percent of staff meeting CPE requirements	12
Number of professional organization meetings attended	3
Number of hours of training per staff	16
Percent staff turnover	9
Others (please list with benchmarks as applicable)	5

Efficiency

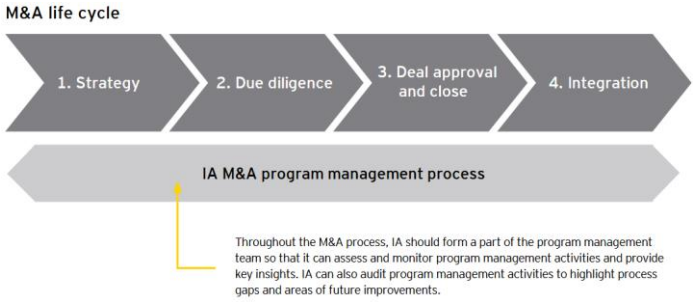
Performance Measure	Responses
Cost per audit hour	3
Dollars spent per dollar audited	3
Hours spent vs. hours budgeted	16
Percent administrative time	14
Time cycle for issuing draft report	13
Number of repeat findings	1
Time cycle for development of annual audit plan	4
Percent of recommendations implemented	11
Others (please list with benchmarks as applicable)	8

Impact

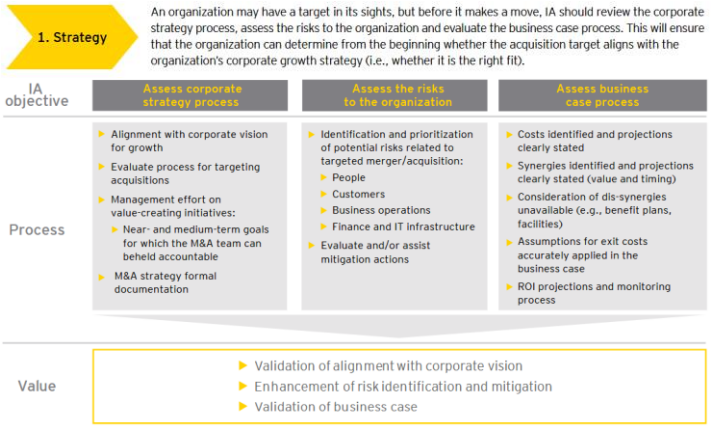
Performance Measures	Responses
Percent of budget audited	9
Percent of identified risks audited	6
Others (please list with benchmarks as applicable)	6

Audit Acquisitions

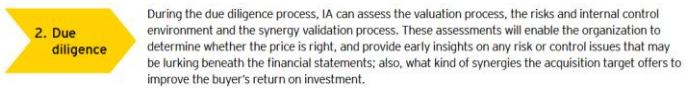
Life Cycle

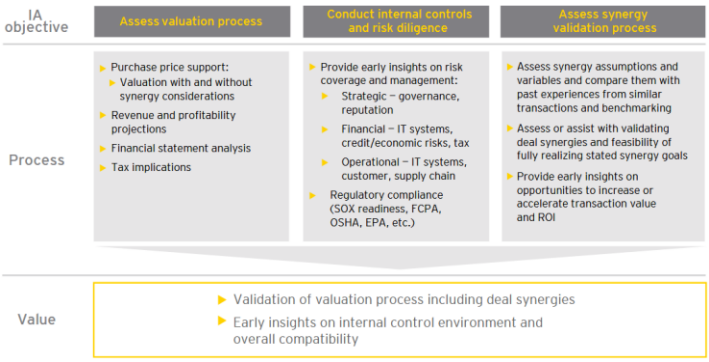


Strategy



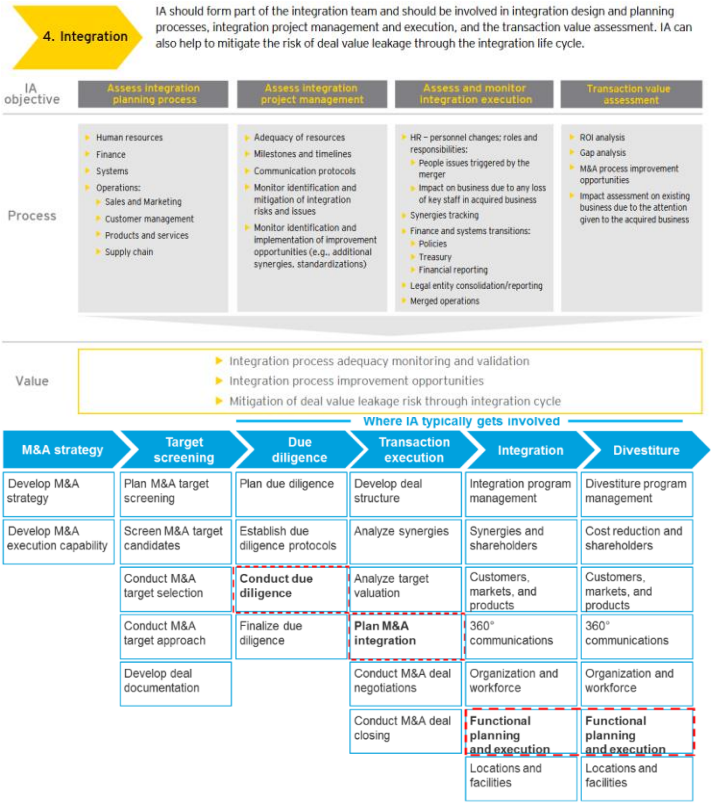
Due Diligence





Deal Approval and Close

Integration



Audit Agile Projects

Audit data: ❶**Development**. Ensure it is planned using agile planning / continuous integration; changes are communicated across teams; environments appropriate & available timely; watch rework following redesign / after bug fixing; watch process to get customer or business change into an assessment: how fast? barriers and points where project fails to perform ❷**Design**. Ensure there IS a design process, no programming hacking without design considerations, design is shared, is performed in agile, change is performed, change is welcomed and encouraged where necessary, daily meetings record element of design changes sufficient for audit ❸**Management**. Ensure delivered using agile approach, commitments are examined, daily meetings taking place, assessments being performed, teams engaged, manager regularly examining team, coaching taking place, all management stakeholders are in place, communicating their commitment, and team is delivering in high performance manner ❹**Process**. Understand if commitments made at the outset are being maintained. Examine how well the agile approach is improving the performance of the project delivery environment and therefore the organisation. **Auditing Guidelines** ❶Audit be non-intrusive ❷Audit not trigger creation of for-Auditor-only documents ❸Generic Scrum checklist tailored to project requirements as basis for audit ❹Auditor is assigned to an entire Sprint per Internal Audit Plan ❺Auditor silent observer of Sprint ❻Auditor added to team mailing list to receive all communications; provided access to all artifacts; attends Sprint Planning, a few Daily Scrum meetings, Sprint Review, Sprint Retrospective meetings. ❼Auditor not schedule formal audit meetings with team members but seek clarifications from ScrumMaster and/or Product Owner during Sprint. ❽Auditors prepare audit report recording their observations and findings against the items in the checklist. Encouraged to go beyond checklist and provide suggestions for improvement. Audit Report presented to Team preferably immediately after Sprint Retrospective meeting. ❾Non-conformances are addressed in forthcoming Sprints and verified by the Auditor.

Audit AI

Framework Strategy: Does the organization have a defined strategy? Is it investing in AI research and development? Does it have plans in place to identify and address AI threats and opportunities? **AI Components** ❶**AI Governance**: structures, processes, procedures implemented to direct, manage, and monitor the AI activities ❷**Data Architecture and Infrastructure**: how data is accessed data is accessible (metadata, taxonomy, unique identifiers, naming conventions)? Information privacy and security throughout the data lifecycle (data collection, use, storage, destruction)? Roles and responsibilities for data ownership & use throughout the data lifecycle? ❸**Data Quality**: completeness, accuracy, and reliability of the data on which AI algorithms are built ❹**AI Performance** ❺**Human Factor**: Risk of unintended human biases factored into AI design is identified and managed ? AI tested to ensure that results reflect the original objective? AI technologies can be transparent given the complexity involved? AI output is being used legally, ethically, responsibly ❻**Black Box Factor**: Type III/Type IV AI technologies — utilizing machines or platforms that can learn on their own or communicate with each other

Audit Big Data

Stakeholders

Project sponsor
Executive level resource who drives support and funding for the program.

Business/data owners
Data owners who support data consolidation and integration into one solution that supports organizational goals.

Business analysts
The resources who maintain knowledge of business needs and technology capabilities in order to transform business requirements into big data solutions.

Consumers (e.g., marketing)
Any function within the organization that consumes data and\or uses the analytic results.

Chief information officer
Executive level resource responsible for delivering the technology solution, as well as partnering with external vendors when big data is outsourced.

Chief privacy officer/chief information security officer
Executive level resources who should be consulted on controls related to the security, protection, and use of the data and resulting analytics.

Chief data officer
Executive level resource who directs enterprise-level data governance.

Technical data analytics resources/data analysts
These resources can include database administrators, software developers, technical tools administrators, and script writers.

Data scientist
An advanced analytics professional who understands the technology and business processes, and can develop and support innovative analytics to drive business value (e.g., predictive analytics).

Risk and Control

Program governance

Key Risk: Lack of appropriate management support, funding, and/or governance over big data program can expose org. to undue risk or failure to meet strategic goals

Control Activities

- Funding should be adequate to support business needs.
- Program objectives should support enterprisewide strategy initiatives.
- Management should receive metrics that demonstrate achievement of goals.
- The organization should establish a governing entity to manage the big data strategy.
- There should be agreed-upon SLAs between the business and IT to describe and measure performance expectations.
- Business and technical requirements should be documented, analyzed, and approved.
- Executive management should develop big data strategy that provides solutions across org.
- Prior to approving the business case, management should conduct a proof of concept to validate that the systems designs align with strategic goals.
- Roles and responsibilities should be clear and well defined.
- Organization should provide necessary resources to deploy and maintain the big data strategy.
- Third-party vendor management best practices should be used to manage big data suppliers.

Technology availability and performance

Key Risk: Ineffective technology solutions and/or configurations may result in a negative customer experience, reduced system availability, and/or degraded performance.

Control Activities

- IT operations should be structured in a manner that supports big data service level expectations.
- Data lifecycle policies and procedures should be documented and followed.
- Big data systems should be part of the maintenance strategy.
- Big data systems should be part of the change management strategy.
- Big data systems should be included in the patch management strategy.
- Big data systems should be procured, built, and/or configured in alignment with the complexity and demands documented in the business case.
- Systems and support tools should be configured to provide automatic notifications to support personnel.
- Reporting tools should be configured to be flexible, intuitive, and easy to use; and training aids should be provided.
- Big data systems should be configured to allow flexibility and scalability without sacrificing performance.
- Periodic performance testing should be conducted and weaknesses should be remediated.
- The big data systems lifecycle should be managed properly.
- IT general controls should be assessed periodically

Security and privacy

Key Risk: Ineffective information security standards and configurations may result in unauthorized access to/ theft of data, inappropriate modifications of data, and regulatory compliance violations

Control Activities

- Information security management should be part of the big data strategy.
- Data security management should be part of the big data strategy.
- Third-party access should be managed properly.
- Data privacy should be part of the big data strategy

Data quality, management, and reporting

Key Risk: Data quality issues and/or inaccurate reporting may lead to inaccurate management reporting and flawed decision making.

Control Activities

- Policies and procedures should be established to ensure data quality.
- Policies and procedures should be established to ensure that data obtained from third parties complies with data quality standards.
- Policies and procedures should be established to ensure reporting accuracy.
- Access to reports should be granted based on business needs.
- Reporting tools and procedures should allow for flexibility and ad-hoc reporting.
- Users should be trained periodically to maximize report utility.
- Selection of vendors who provide reporting products & services should align with business needs

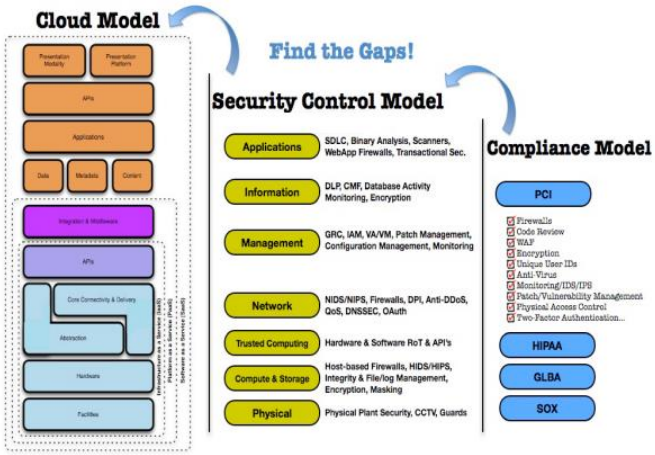
Audit Cloud

Cloud Characteristic	Potential Audit concern
On Demand Self Service	• User driven versus IT driven • Shadow IT • Cloud Services discovery
Broad Network Access	• Enhanced threat profile, attack surface • Perimeter definition
Resource Pooling	• Multi-tenancy • Co-mingling of data and assets
Rapid Elasticity	• VM Sprawl- uncontrolled scale up • Data Remanance
Measured Service	• Proliferation of cloud services due to initial low opex

Cloud Risks

Policy & Organisational Risk	• Provider Lock in • Loss of Governance • Compliance Risk • Provider Exit
Technical Risks	• Consolidation of IT Infrastructure – single point of failure • Control over technical risk shifting to provider • Insecure or incomplete data deletion •Lack of Portabilty
Virtualisation Risks	• Guest Escape – Break out of OS – Access by Hypervisor or other guests • Sprawl – Loss of control over image store • Multitenancy
Legal Risks	• Data Protection
Non Cloud Specific Risks	• Natural disasters • Unauthorised facility access

Security Controls



Auditing SAAS

•Customisable reports •Application Functionality Configuration options •Application Security configuration options (aka ERP configurable controls) •User driven data export /interface capabilities •Limited or nil involvement in application development life cycle •CAAT development is challenging •Logs for access controls, Transaction activity, Change management etc. •Existence of myriad of logs •Need automation to map controls to Key Risk Indicators – KRIs •Opportunities to leverage cloud infrastructure - it is more cost effective and efficient to develop on demand , elastic audit databases, implement audit automation

Auditing IaaS & PaaS

Example : Continuous Monitoring services in AWS

AWS CloudTrail
AWS CloudTrail is a service that logs API activity within an AWS account and delivers these logs to an Amazon Simple Storage Service (Amazon S3) bucket.

Amazon CloudWatch
Alarms Amazon CloudWatch alarms notify users and applications when events related to AWS resources occur.

AWS Config AWS Config
AWS Config allows detailed tracking and notification whenever a resource in an AWS account is created, modified, or deleted.

Audit concerns

- Ensure PaaS Portability (open standard APIs)
- New approaches to auditing DevOps (DevOps Control Objectives)
- Audit Automation challenges

- Third party attestation SOC 1/ SOC2

- No physical access to data centre

How can we leverage cloud platform to implement audit automation

Cloud provides unique opportunities for audit automation and audit analytics

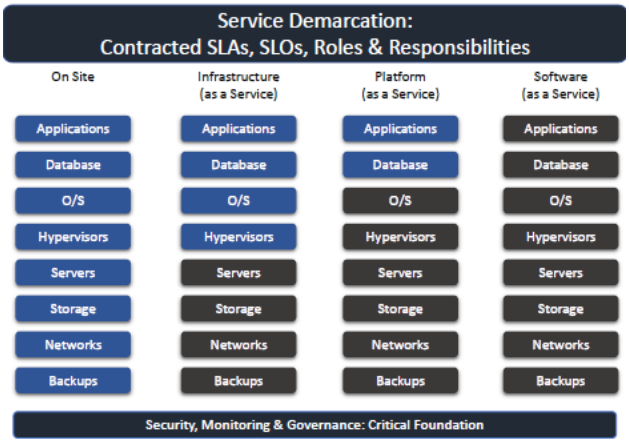
- Ability to create VM instances on demand for analytics
- Measured service, low opex
- Rapid elasticity to address audit universe
- Ability to scale down
- Avoid slow data downloads
- Potential for "in memory" analysis
- Big Data - Hadoop/MapReduce

Context

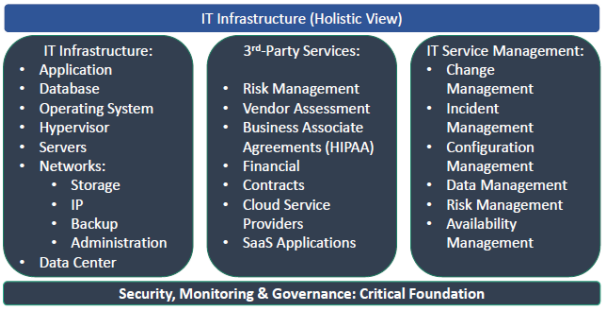
Risks

❶Account lock-out/resource hijacking? ❷Misconfiguration leading to breach (e.g. S3)? ❸Loss of control? ❹Asymmetries between the provider and customer? ❺Comingling of data / multi-tenancy? ❻Jurisdictional? ❼Who should make risk decisions?

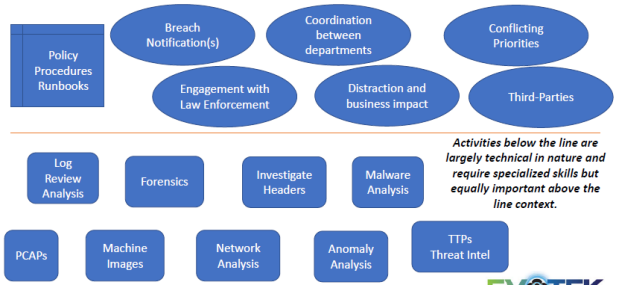
Service Layer



IT Functions



Incident Management



ISACA Audit Cloud

1. PLANNING AND SCOPING THE AUDIT

1.1 Define audit/assurance objectives (high level and describe the overall audit goals)

1.1.1 Review the audit/assurance objectives in the introduction to this audit/assurance program.

1.1.2 Modify the audit/assurance objectives to align with the audit/assurance universe, annual plan and charter.

1.2 Define the boundaries of review. The review must have a defined scope. Understand the core business process and its alignment with IT, in its noncloud form and current or future cloud implementation.

1.2.1 Obtain a description of all cloud computing environments in use and under consideration.

1.2.2 Obtain a description of all cloud computing applications in use and under consideration.

1.2.3 Identify the types of cloud services (IaaS, PaaS, SaaS) in use and under consideration, and determine the services and business solutions to be included in the review.

1.2.4 Obtain and review any previous audit reports with remediation plans. Identify open issues, and assess updates to the documents with respect to these issues.

1.3 Identify and document risk. The risk assessment is necessary to evaluate where audit resources should be focused. The risk-based approach assures utilization of audit resources in the most effective manner.

1.3.1 Identify the business risk associated with cloud computing of concern to business owners and key stakeholders.

1.3.2 Verify that the business risk is aligned, rated or classified with cloud computing security criteria such as confidentiality, integrity and availability.

1.3.3 Review previous audits of cloud computing.

1.3.4 Determine if the risk identified previously has been appropriately addressed.

1.3.5 Evaluate the overall risk factor for performing the review.

1.3.6 Based on the risk assessment, identify changes to the scope.

1.3.7 Discuss the risk with IT management, and adjust the risk assessment.

1.3.8 Based on the risk assessment, revise the scope.

1.4 Define the change process. The initial audit approach is based on the reviewer's understanding of the operating environment and associated risk. As research and analysis are performed, changes to the scope and approach may result.

1.4.1 Identify the senior IT assurance resource responsible for the review.

1.4.2 Establish the process for suggesting and implementing changes to the audit/assurance program and the authorizations required.

1.5 Define assignment success. The success factors need to be identified. Communication among the IT audit/assurance team, other assurance teams and the enterprise is essential.

1.5.1 Identify the drivers for a successful review (this should exist in the assurance function's standards and procedures).

1.5.2 Communicate success attributes to the process owner or stakeholder, and obtain agreement.

1.6 Define the audit/assurance resources required. The audit/assurance resources required for a successful review need to be defined. (Refer to the Minimum Audit Skills section in section V.)

1.6.1 Determine the audit/assurance skills necessary for the review.

1.6.2 Estimate the total audit/assurance resources (hours) and time frame (start and end dates) required for the review.

1.7 Define deliverables. The deliverable is not limited to the final report. Communication between the audit/assurance teams and the process owner about the number, format, timing and nature of deliverables is essential to success.

1.7.1 Determine the interim deliverables, including initial findings, status reports, draft reports, due dates for responses or meetings, and the final report.

1.8 Communications. The audit/assurance process must be clearly communicated to the customer/client.

1.8.1 Conduct an opening conference to discuss: • Review objectives with the stakeholders • Documents and information security resources required to effectively perform the review • Timelines and deliverables

2. GOVERNING THE CLOUD

2.1 Governance and Enterprise Risk Management (ERM)

2.1.1 Governance - Audit/Assurance Objective: Governance functions are established to ensure effective and sustainable management processes that result in transparency of business decisions, clear lines of responsibility, information security in alignment with regulatory and customer organization standards, and accountability.

2.1.1.1 Governance Model - Control: The organization has mechanisms in place to identify all providers and brokers of cloud services with which it currently does business and all cloud deployments that exist across the enterprise. The organization ensures that customer, IT, information security and business units actively participate in the governance and policy activities to align business objectives and information security capabilities of the service provider with those of the organization.

2.1.1.1.1 Determine if the IT, information security and key business functions have defined integrated governance framework and monitoring processes.

2.1.1.1.2 Determine if the IT, information security functions and key business units are actively involved in the establishment of SLAs and contractual obligations.

2.1.1.1.3 Determine if the information security function has performed a gap analysis of the service provider's information security capabilities against the organization's information security policies and threat and vulnerabilities/IT risk emanating from the transition to cloud computing.

2.1.1.1.4 Determine if the cloud provider has identified control objectives for the provided services.

2.1.1.1.5 Determine if the organization maintains an inventory of all services provided via the cloud.

2.1.1.1.6 Determine that the business cannot procure cloud services without the involvement of IT and information security.

2.1.1.2 Information Security Collaboration - Control: Both parties define reporting relationship and responsibilities.

2.1.1.2.1 Determine if governance responsibilities documented & approved by service provider & customer.

2.1.1.2.2 Determine if reporting relationships between the service provider and customer are clearly defined, identifying the responsibilities of both organizations' governance processes.

2.1.1.3 Metrics and SLAs - Control: SLAs that support the business requirements are defined, accepted by the service provider and monitored.

2.1.1.3.1 Obtain the SLAs; determine if the SLAs reflect the business requirements.

2.1.1.3.2 Determine that the SLAs can be monitored using measurable metrics and that the metrics provide appropriate oversight and early warning of unacceptable performance.

2.1.1.3.3 Determine if SLA contains clauses for services when vendor acquisition/ changes in management

2.1.2 Enterprise Risk Management - Audit/Assurance Objective: Risk management practices are implemented to evaluate inherent risk within the cloud computing model, identify appropriate control mechanisms, and ensure that residual risk is within acceptable levels.

2.1.2.1 Identification of Risk - Control: The risk management process provides a thorough assessment of the risk to the business by implementing the cloud processing model and is aligned to ERM if applicable.

2.1.2.1.1 Determine if the organization has an ERM model.

2.1.2.1.2 If an ERM model has been implemented, determine if the cloud computing risk assessment is in alignment with the enterprise ERM.

2.1.2.1.3 Determine if the services provided by the service provider and the processing model selected will limit the availability or execution of required information security activities: • Restrictions on vulnerability assessments and penetration testing • Availability of audit logs • Access to activity monitoring reports • Segregation of duties

2.1.2.1.4 Determine if the risk management approach includes the following: • Identification and valuation of assets and services • Identification and analysis of threats and vulnerabilities with their potential impact on assets • Analysis of the likelihood of events using a scenario approach • Documented management approval of risk acceptance levels and criteria • Risk action plans (control, avoid, transfer, accept)

2.1.2.1.5 Determine if, during the risk assessment, the identified assets include both service-provider- and customer-owned assets and if the information security classifications used in the risk assessments are aligned.

2.1.2.1.6 Determine if the risk assessment includes the service model and the service provider's capabilities and financial condition

2.1.2.2 Integration of Risk and SLAs - Control: SLAs are aligned and developed in conjunction with the results of the risk assessment.

2.1.2.2.1 Determine if the results of the risk action plans are incorporated into the SLAs.

2.1.2.2.2 Determine if a joint service provider/customer risk assessment was conducted to verify if all reasonable risk has been identified and if risk remediation alternatives were identified and documented.

2.1.2.2.3 Where the risk assessment of the service provider has identified risk management that is either ineffective or not comprehensive, determine if the organization has performed an analysis of their compensating controls and if such controls will address the service provider's control shortcomings.

2.1.2.3 Acceptance of Risk - Control: Risk acceptance is approved by a member of management with the authority to accept the risk on behalf of the organization and who understands the implications of the decision.

2.1.2.3.1 Determine if management has performed an analysis of their quantification and acceptance of residual risk prior to implementing a cloud solution.

2.1.2.3.2 Determine if the individual accepting such risk has the authority to make this decision.

2.1.3 Information Risk Management - Audit/Assurance Objective: A process to manage information risk exists and is integrated into the organization's overall ERM framework. Information risk management information and metrics are available for the information security function to manage risk within the risk tolerance of the data owner.

2.1.3.1 R isk Management Framework and Maturity Model - Control: A risk management framework and a maturity model have been implemented to quantify risk and assess the effectiveness of the risk model.

2.1.3.1.1 Determine if a risk framework has been identified and approved.

2.1.3.1.2 Determine if a maturity model is used to assess the effectiveness.

2.1.3.1.3 Review the results of the maturity model results, and determine if the lack of maturity materially affects the audit objectives.

2.1.3.2 Risk Management Controls - Control: Risk management controls are in effect to manage risk-based decisions.

2.1.3.2.1 Identify the technology controls and contractual requirements necessary to make fact-based information risk decisions. Consider: • Information usage • Access controls • Security controls • Location management • Privacy controls

2.1.3.2.2 For SaaS, determine that the organization has identified analytical information required from the service provider to support contractual obligations relating to performance, security and attainment of SLAs.

2.1.3.2.3 Obtain the analytical data requirements, and determine if the organization routinely monitors and evaluates the attainment of SLAs.

2.1.3.2.4 For PaaS, determine that the organization has identified the information available and the control practices necessary to manage the application and development processes effectively that address availability, confidentiality, data ownership, concerns around e-discovery, privacy and legal issues.

2.1.3.2.5 Determine if the organization has established monitoring practices to identify risk issues.

2.1.3.2.6 For IaaS, determine that the organization has identified and monitors the control and security processes necessary to provide a secure operating environment.

2.1.3.2.7 Determine if the service provider makes available metrics and controls to assist customers in implementing their information risk management requirements.

2.1.4 Third-party Management - Audit/Assurance Objective: The customer recognizes the outsourced relationship with the service provider. The customer understands its responsibilities for controls, and the service provider has provided assurances of sustainability of those controls.

2.1.4.1 Service Provider Procedures - Control: The service provider makes available to customers independent third-party assessments, using generally accepted audit procedures, to describe the control practices in place at the service provider's operating locations.

2.1.4.1.1 Determine if the service provider routinely has independent third-party assessments performed and issued.

2.1.4.1.2 Determine if the scope of the third-party assessment includes descriptions of the following service provider processes: • Incident management • Business continuity and disaster recovery • Backup and co-location facilities

2.1.4.1.3 Determine if the service provider routinely performs internal assessments of conformance to its own policies, procedures and availability of control metrics.

2.1.4.2 S ervice Provider Responsibilities - Control: The service provider has established processes to align its operations with requirements of the customer.

2.1.4.2.1 Determine if the service provider's information security governance, risk management and compliance processes are routinely assessed and include: • Risk assessments and reviews of facilities and services for control weaknesses • Definition of critical service and information security success factors and key performance indicators • Frequency of assessments • Mitigation procedures to ensure timely completion of identified issues • Review of legal, regulatory, industry and contractual requirements for comprehensiveness • Cloud service provider's oversight of risk from its own critical vendors • Terms of use due diligence to identify roles, responsibilities and accountability of the service provider • Legal review for local contract provisions, enforceability and laws pertaining to jurisdictional issues that are the responsibility of their service provider

2.1.4.3 Customer Responsibilities - Control: The customer performs due diligence processes to ensure sustainability and compliance with regulatory requirements.

2.1.4.3.1 Determine if the customer has performed due diligence with respect to the service provider's information security governance, risk management and compliance processes as described under 2.1.4.2 Service Provider Responsibilities.

2.1.4.3.2 Determine if the customer has prepared for the loss of service provider services: • A business continuity and disaster recovery plan for various processing interruption scenarios • Tests of business continuity and disaster plan • Inclusion of the business users and their business impact analysis in the continuity plan

2.2 Legal and Electronic Discovery

2.2.1 Contractual Obligations - Audit/Assurance Objective: The service provider and customer establish bilateral agreements and procedures to ensure contractual obligations are satisfied, and these obligations address the compliance requirements of both the customer and service provider.

2.2.1.1 Contract Terms - Control: A contract team representing customer's legal, financial, information security and business units has identified and included contractual issues in the contract from the customer's perspective, and the service provider's legal team has provided contractual assurance to the satisfaction of the customer.

2.2.1.1.1 Determine if the contractual agreement defines both parties' responsibilities related to discovery searches, litigation holds, preservation of evidence and expert testimony.

2.2.1.1.2 Determine that the service provider contract requires assurance to the customer that their data are preserved as recorded, including the primary data and secondary information (metadata and logs).

2.2.1.1.3 Determine that service providers understand their contractual obligations to provide guardianship of the customer's data. Review contracts to determine this is specifically addressed.

2.2.1.1.4 Determine that the customer's duty of care includes full scope of contract monitoring, including: • Precontract due diligence • Contract term negotiation • Transfer of data custodianship • Contract termination or renegotiation • Transition from processing

2.2.1.1.5 Determine that the contract stipulates and both parties understand their obligations for both expected and unexpected termination of the relationship during and after negotiations and that the contract and/or precontract agreement provides for the orderly and timely return or secure disposal of assets.

2.2.1.1.6 Determine that the contractual obligations specifically identify suspected data breach responsibilities of both parties and cooperative processes to be implemented during the investigation and any follow-up actions.

2.2.1.1.7 Determine that the agreement provides for the customer to have access to the service provider's performance and tests for vulnerabilities on a regular basis.

2.2.1.1.8 Determine that the contract establishes rights and obligations for both parties during transition at the conclusion of the relationship and after the contract terminates.

2.2.1.1.9 Determine if the contract establishes the following data protection processes: • Full disclosure of the service provider's internal security practices and procedures • Data retention policies in conformance with local jurisdiction requirements • Reporting on geographical location of customer data • Circumstances in which data can be seized and notification of any such events • Notification of subpoena or discovery concerning any customer data or processes • Penalties for data breaches • Protection against data contamination between customers (compartmentalization)

2.2.1.1.10 Encryption requirements for data in transit, at rest and for backup are clearly identified in the cloud contractual agreement.

2.2.1.2 Implementation of Contractual Requirements - Control: The customer has implemented appropriate monitoring controls to ensure contractual obligations are satisfied.

2.2.1.2.1 Determine that the customer has considered and established controls within the contractual obligations to ensure retention of data and intellectual property ownership and the privacy of personal data contained within its data.

2.2.1.2.2 Determine that the customer has developed appropriate issue monitoring processes to oversee the service provider's performance of contract requirements.

2.2.1.2.3 Determine that the customer has established internal issue monitoring to identify customer contractual compliance deficiencies.

2.2.2 L egal Compliance - Audit/Assurance Objective: Legal issues relating to functional, jurisdictional and contractual requirements are addressed to protect both parties, and these issues are documented, approved and monitored.

2.2.2.1 Legal Compliance - Control: Legal compliance to local and cross-border laws are defined as a component of the contract.

2.2.2.1.1 Determine if cross-border and local laws are defined and considered in the contract

2.2.2.1.2 Determine if the service provider and customer have an agreed-upon unified process for responding to subpoenas, service of process, and other legal requests.

2.3 Compliance and Audit

2.3.1 Right to Audit - Audit/Assurance Objective: The right to audit is clearly defined and satisfies the assurance requirements of the customer's board of directors, audit charter, external auditors and any regulators having jurisdiction over the customer.

2.3.1.1 Audit Rights per Contract - Control: The audit rights, as agreed in the contract, permit the customer to conduct professional control assessments.

2.3.1.1.1 Review the audit rights in the contract, and determine if audit activities can be restricted or curtailed by the service provider.

2.3.1.1.2 If audit rights issues are identified, prepare an appropriate summary of the findings and escalate to service provider relationship management. If necessary and appropriate, escalate to the audit committee.

2.3.1.2 Third-party Reviews - Control: The service provider submits third-party reviews that satisfy the professional requirements of being performed by a recognized independent audit organization. The report describes the controls in place by the service provider and certifies that the controls have been tested using recognized selection criteria. A test period previously agreed upon provides a description of recommended customer and service provider responsibilities and controls.

2.3.1.2.1 Obtain the third-party report.

2.3.1.2.2 Determine that the report addresses the control environment utilized by the customer.

2.3.1.2.3 Determine that the descriptions and processes are relevant to the service provider's customers.

2.3.1.2.4 Determine that the report has described the key controls necessary for the reviewer to assess compliance with appropriate control objectives.

2.3.1.2.5 Determine that the report and testing will satisfy the customer's assurance charter and compliance requirements of all regulators having jurisdiction over the customer.

2.3.1.2.6 Using the approved customer audit universe, compare the scope of the audit universe to the scope of the third-party report; identify gaps in the latter requiring additional assurance coverage.

2.3.1.2.7 Determine if the service provider relationship crosses international boundaries and if this affects the ability to rely upon the third-party report.

2.3.2 Auditability - Audit/Assurance Objective: The service provider's operating environment should be subject to audit to satisfy the customer's audit charter, compliance requirements and good practice controls without restriction.

2.3.2.1 Customer Assurance Reviews of Service Provider Processes - Control: The customer performs appropriate reviews to supplement and/ or replace third-party reviews as required by their audit universe and audit charter.

2.3.2.1.1 Determine if supplementary assurance assessments (if a third-party review has been provided) or primary assurance assessments are required

2.3.2.1.2 Generate appropriate requests to the service provider, and schedule reviews. Note: Utilize appropriate audit/assurance programs for these reviews.

2.3.3 Compliance Scope - Audit/Assurance Objective: The use of cloud computing does not invalidate or violate any customer compliance agreement.

2.3.3.1 Feasibility of Data Security Compliance - Control: Data regulations are identified by compliance topic and are mapped to the regulator's requirements. Gaps are evaluated to determine if the cloud computing platform will invalidate or breach compliance requirements.

2.3.3.1.1 Determine if the customer has identified the legal and regulatory requirements of which it must comply (i.e., EU Data Directive, PCAOB AS5, PCI DSS, HIPAA).

2.3.3.1.2 Determine if the customer has aggregated requirements to minimize duplication.

2.3.3.1.3 Using the documentation assembled in the Governance and Enterprise Risk Management, Legal and Electronic Discovery, and Right to Audit sections, perform a gap analysis against the data regulations to determine if there are any regulatory requirements that cannot be satisfied by the cloud computing model.

2.3.3.2 Data Protection Responsibilities - Control: The deployment scenario (IaaS, PaaS, SaaS) defines the data protection responsibilities between the customer and service provider, and these responsibilities are clearly established contractually.

2.3.3.2.1 Determine that the responsibilities for data protection are based on the risk for the deployment scenario.

2.3.3.2.2 Review the contract to determine the assignment of responsibilities.

2.3.3.2.3 Based on the contract, determine if the customer and service provider each have established appropriate data protection measures within the scope of their responsibilities.

2.3.4 ISO 27001 Certification - Audit/Assurance Objective: Service provider security assurance is provided through ISO 27001 Certification.

2.3.4.1 ISO Information Security Certification - Control: ISO 27001 certification provides assurance of the service provider's adherence to best-practice security processes.

2.3.4.1.1 Determine if the service provider has received ISO 27001 certification. If so, adjust the scope of the audit/assurance program to reflect this certification.

2.4 Portability and Interoperability

2.4.1 Service Transition Planning - Audit/Assurance Objective: Planning for the migration of data, such as formats and access, is essential to reducing operational and financial risk at the end of the contract. The transition of services should be considered at the beginning of contract negotiations.

2.4.1.1 Portability - Control: Procedures, capabilities and alternatives are established, maintained and tested, and a state of readiness has been established to transfer cloud computing operations to an alternate service provider in the event that the selected service provider is unable to meet contractual requirements or ceases operations.

2.4.1.1.1 All cloud solutions

2.4.1.1.1.1 Determine that the hardware and software requirements and feasibility for moving from the existing service provider (legacy provider) to another provider (new provider) have been documented for each cloud computing initiative.

2.4.1.1.1.2 Determine that an alternate service provider for each legacy service provider has been identified and that the feasibility for transferring processes has been evaluated.

2.4.1.1.1.3 Determine if the feasibility analysis includes procedures and time estimates to move large volumes of data, if applicable.

2.4.1.1.1.4 Determine if the portability process has been tested.

2.4.1.1.2 IaaS cloud solutions

2.4.1.1.2.1 Determine if the feasibility analysis of transferring from the IaaS legacy service provider involves any proprietary functions or processes that would preclude or delay the transferring of operations.

2.4.1.1.2.2 Determine if the portability analysis includes processes to protect the intellectual property and data from the legacy service provider once the transfer has been completed.

2.4.1.1.3 PaaS cloud solutions

2.4.1.1.3.1 Determine if the feasibility analysis includes identification of application components and modules that are proprietary and would require special programming during transfer.

2.4.1.1.3.2 Determine if the portability analysis includes: • Translation functions to a new service provider • Interim processing until a new service provider is operational • Testing of new processes before promotion to a production environment at the new service provider

2.4.1.1.4 SaaS cloud solutions

2.4.1.1.4.1 Determine if the portability analysis includes:

• A plan to back up the data in a format that is usable by other applications • Routine backup of data • Identification of custom tools required to process the data and plans to redevelop • Testing of the new service provider's application and due diligence before conversion

3. OPERATING IN THE CLOUD

3.1 Incident Response, Notification and Remediation

Audit/Assurance Objective: Incident notifications, responses, and remediation are documented, timely, address the risk of the incident, escalated as necessary and are formally closed.

3.1.1 Incident Response - Control: The contract SLAs describe specific definitions of incidents (data breaches, security violations) and events (suspicious activities) and the actions to be initiated by and the responsibilities of both parties.

3.1.1.1 Obtain and review the SLAs per the contract to determine that incidents and events are clearly defined and responsibilities assigned.

3.1.1.2 Review cooperation agreements, and evaluate the responsibilities for the investigation of incidents.

3.1.1.3 Notification procedures according to local laws are incorporated into the incident and event process.

3.1.2 Service Provider Issue Monitoring - Control: Issue monitoring processes are implemented and actively used by the service provider to document and report all defined incidents.

3.1.2.1 Obtain and review the service provider's issue monitoring procedures.

3.1.2.2 Determine if the monitored reporting requirements are aligned with the customer's incident reporting policy.

3.1.2.3 Obtain the incident monitoring reports for a representative period of time.

3.1.2.3.1 Determine that the: • Customer was notified of the incident within the SLA requirements • Remediation was timely based on the scope and risk of the incident • Remediation was appropriate • Issue was escalated, if appropriate • Issue was closed and the customer notified in a timely manner

3.1.3 Customer Issue Monitoring - Control: The customer has established an issue monitoring process to track internal and service provider incidents.

3.1.3.1 Obtain the customer incident monitoring procedure.

3.1.3.2 Determine if the incident monitoring procedure tracks both internal and service provider incidents.

3.1.3.3 Select a sample of incidents, and determine that: • The service provider notified the customer on a timely basis within scope of the contract. • The remediation was timely based on the scope and risk of the incident. • The remediation was appropriate. • The issue was escalated within the service provider's hierarchy. • The issue was closed by the service provider. • The issue was monitored and reported to customer management. • Customer procedures were modified to recognize the increased risk. • Internal customer incidents were recorded by the customer, appropriately reported, remediated and closed.

3.2 Application Security

3.2.1 Application Security Architecture - Audit/Assurance Objective: Applications are developed with an understanding of the interdependencies inherent in cloud applications, requiring a risk analysis and design of configuration management and provisioning process that will withstand changing application architectures.

3.2.1.1 Application Security Architecture - Control: The design of cloud-based applications includes information security and application security architecture subject matter experts, and the process focuses on the interdependencies inherent in cloud applications.
3.2.1.1.1 Obtain the application design documentation, and review the policies for subject matter expert involvement in the system design.
3.2.1.1.2 Determine that information security and architecture specialists have been fully engaged during the planning and deployment of cloud applications.
3.2.1.1.3 Select recent implementations, and review the project and development plans for evidence of information security and subject matter expert involvement.
3.2.1.2 Configuration Management and Provisioning - Control: Configuration management and provisioning procedures are segregated from the service provider, limited to a security operations function within the customer's organization and provide audit trails to document all activities.
3.2.1.2.1 Obtain the configuration management and provisioning security architecture.
3.2.1.2.2 Determine if the service provider is prevented from configuring or provisioning users (both administrative and standard users), which may affect data integrity, access or security.
3.2.1.2.3 Determine if logs and audit trails exist, record these activities and how they are monitored and reviewed.
3.2.2 Compliance - Audit/Assurance Objective: Compliance requirements are an integral component of the design and implementation of the application security architecture.
3.2.2.1 Compliance - Control: The SDLC includes processes to ensure compliance requirements are identified, mapped to the cloud-based application, and included in the final product. Compliance gaps are escalated to appropriate senior management for waiver approval.
3.2.2.1.1 Obtain compliance analysis utilized as basis for authorizing the initiation of a cloud-based application.
3.2.2.1.2 Determine if a formal compliance review is performed and if senior management authorization is required where internal information security policies require a waiver to allow the implementation of the cloud-based application.
3.2.3 Tools and Services - Audit/Assurance Objective: Use of development tools, application management libraries and other software are evaluated to ensure their use will not negatively impact the security of applications.
3.2.3.1 Tools and Services - Control: All tools and services used in the development, management and monitoring of applications are itemized and the ownership documented, and their effect on the security of the application is explicitly analyzed. High-risk tools and services are escalated to senior information management for approval.
3.2.3.1.1 Obtain an analysis of tools and services in use.
3.2.3.1.2 Determine if the ownership of each tool and service has been identified.
3.2.3.1.3 Determine if information security risk was evaluated for each tool and service. If one is deemed a security risk, determine the disposition (escalation, waiver to use or disallow use of software in a cloud environment).
3.2.3.1.4 Examine examples of escalated requests, and determine the adherence to procedures.
3.2.4 Application Functionality - Audit/Assurance Objective: For SaaS implementations, the application outsourced to the cloud contains the appropriate functionality and processing controls required by the customer's control policies within the processing scope (financial, operational, etc.).
3.2.4.1 Application Functionality - Control: The application functionality is subject to an assurance review as part of the customer's application process assurance audit.
3.2.4.1.1 Refer to a standard application audit program for specific steps.

3.3 Data Security and Integrity

3.3.1 Encryption - Audit/Assurance Objective: Data are securely transmitted and maintained to prevent unauthorized access and modification.
3.3.1.1 Data in Transit - Control: Data in transit are encrypted over networks with private keys known only to the customer.
3.3.1.1.1 Obtain the encryption policies and procedures for data in transit
3.3.1.1.2 Evaluate if the encryption processes include the following: • Classification of data traversing cloud networks (top secret, confidential, company confidential, public) • Encryption technologies in use • Key management (see key management analysis in section 3.3.2) • A list of external organizations of the customer that have decryption keys to data in transit
3.3.1.2 Data at Rest - Control: Data stored in live production databases on cloud systems are encrypted, with knowledge of the decryption keys limited to the customer.
3.3.1.2.1 Obtain the encryption policies and procedures for data stored on cloud systems.
3.3.1.2.2 For SaaS implementations, determine if the service provider has implemented data at rest encryption.
3.3.1.2.3 Determine if sensitive data need to be exclusively stored on customer systems to satisfy customer policy, regulatory or other compliance requirements.
3.3.1.2.4 Evaluate if the encryption processes include the following: • Classification of data stored on cloud networks (top secret, confidential, company confidential, public) • Encryption technologies in use • Key management (see key management analysis section 3.3.2) • A list of external organizations of the customer that have decryption keys to data at rest
3.3.1.3 Data Backup - Control: Data backups are available encrypted.
3.3.1.3.1 Obtain data backup policies and procedures for data backups of cloud-based data.
3.3.1.3.2 Determine if data are encrypted to prevent unauthorized access and disclosure of confidential data.
3.3.1.3.3 Determine if the encryption key structure provides adequate data confidentiality.
3.3.1.3.4 Assess if backup processes provide the ability to restore configurations and data for a predetermined period to allow for forensic and other evaluation activities.
3.3.1.3.5 Determine if tests of data restoration are performed on a routine basis.
3.3.1.4 Test Data Confidentiality - Control: Test data do not contain and are prohibited from using copies of any current or historical production data containing sensitive/confidential information.
3.3.1.4.1 Obtain testing policies and standards.
3.3.1.4.2 Determine if policies specifically exclude the use of any current or historical production data.
3.3.1.4.3 Perform sampling procedures to determine compliance with the test data prohibition policy.
3.3.2 Key Management - Audit/Assurance Objective: Encryption keys are securely protected against unauthorized access, separation of duties exists between the key managers and the hosting organization, and keys are recoverable.
3.3.2.1 Secure Key Stores - Control: The key stores are protected during transmission, storage and back up.
3.3.2.1.1 Obtain an understanding of how the key stores are protected.
3.3.2.1.2 Evaluate access controls, transmission controls and backup to ensure that the key stores are in the possession of the key managers.
3.3.2.1.3 Identify potential access breaches to key stores, and identify compensating controls.
3.3.2.2 Access to Key Stores - Control: Key stores access is limited to the key managers whose jobs are separated from the process the key stores protect.
3.3.2.2.1 Identify the key store managers.
3.3.2.2.2 Perform a separation of duties analysis to determine the specific functional transactions to which the key store managers have access.
3.3.2.2.3 Evaluate if the positions of key store managers and their access to key stores creates a vulnerability to data confidentiality or integrity.
3.3.2.2.4 Determine if the service provider has access to the keys and has the procedures and oversight to ensure the confidentiality of customer data.
3.3.2.2.5 Determine if appropriate controls protect the keys during generation and disposal.
3.3.2.3 Key Backup and Recoverability - Control: Key backup and recoverability have been established and tested to ensure continued access to data keys.
3.3.2.3.1 Obtain the backup and recovery policies and procedures.
3.3.2.3.2 Perform a risk assessment, with known vulnerabilities, to determine that the key backups would be available and recovery would be assured.
3.3.2.3.3 Determine if a key recovery test process exists and is routinely executed.
3.3.2.3.4 Review recent key recovery tests. Evaluate the validity of each test, the analysis and remediation process used, and the preparedness for key restoration.

3.4 Identity and Access Management

3.4.1 Identity and Access Management - Audit/Assurance Objective: Identity processes assure only authorized users have access to the data and resources, user activities can be audited and analyzed, and the customer has control over access management.
3.4.1.1 Identity Provisioning - Control: User provisioning (on-boarding), deprovisioning (termination) and job function changes of cloud-based applications and operating platforms are managed in a timely and controlled manner, according to internal user access policies.
3.4.1.1.1 Obtain internal provisioning/deprovisioning policies.
3.4.1.1.2 Analyze provisioning/deprovisioning policies in relation to procedures implemented for cloud systems.
3.4.1.1.3 Using the identity management section of the ISACA Identity Management Audit/Assurance Program, identify gaps in controls that require additional focus.
3.4.1.2 Authentication - Control: Responsibility for user authentication remains with the customer; single sign on and open authentication (as opposed to service provider proprietary authentication technologies) should be used.
3.4.1.2.1 For SaaS and PaaS, determine if the customer can establish trust between the internal authentication system and the cloud system.
3.4.1.2.2 Determine, where there is an option, that the nonproprietary authentication process has been implemented at the service provider.
3.4.1.2.3 If a proprietary authentication process is the only option, determine if appropriate controls are in place to: • Prevent shared user IDs • Provide adequate separation of duties to prevent service provider staff from obtaining customer identities • Provide forensic and logging functions to provide history of activities • Provide monitoring functions to alert customer of unauthorized authentication activities
3.4.1.2.4 For IaaS: • If dedicated VPNs are implemented between the service provider and customer installations, determine if the users are authenticated at the customer network before passing transactions through the VPN. Dedicated VPNs are implemented between the service provider and customer installations to authenticate users at the customer network before passing transactions along through the VPN. • Where a dedicated VPN is not feasible, determine if recognized standard authentication formats are in use (e.g., SAML, WS-Federation) in conjunction with SSL.
3.4.1.2.5 For IaaS and private, internal cloud deployments, verify that third-party access control solutions operate effectively in virtualized and cloud environments and that event data can be aggregated and correlated effectively for management review.
3.4.1.2.6 Using the authentication section of the ISACA Identity Management Audit/Assurance Program, identify gaps in controls that require additional focus.

3.5 Virtualization

3.5.1 Virtualization - Audit/Assurance Objective: Virtualization operating systems are hardened to prevent cross-contamination with other customer environments.
3.5.1.1 Virtualization - Control: Operating system isolation and security controls are implemented by the service provider to prevent unauthorized access and attacks.
3.5.1.1.1 Identify the virtual machine configuration in place.
3.5.1.1.2 Determine if additional controls have been implemented, including the following: • Intrusion detection • Malware prevention • Vulnerability scanning • Baseline management and analysis • Virtual machine image validation prior to placement in production • Preclude bypassing security mechanisms by the identification of security-related APIs in use • Separate production and testing environments • Internal organization identity management for administrative access • Timely isolation intrusion reporting

Audit Cyber Security

NIST Cybersecurity Framework

Figure 7—NIST Initial Framework Considerations

Categories	Framework Principles	Common Points	Initial Gaps
Themes	• Flexibility • Impact on global operations • Risk management approaches • Leverage existing approaches, standards and best practices	• Senior management engagement • Understanding threat environment • Business risk/risk assessment • Separation of business and operational systems • Models/levels of maturity • Incident response • Cybersecurity workforce	• Metrics • Privacy/civil liberties • Tools • Dependencies • Industry best practices • Resiliency • Critical infrastructure cybersecurity nomenclature

Source: NIST, *2013 Initial Analysis of Cybersecurity Framework RFI Responses*, USA, figure 1, *http://csrc.nist.gov/cyberframework/nist-initial-analysis-of-rfi-responses.pdf*

CSF vs. COBIT

CSF Implementation Steps	COBIT 5 Principles
Step 1: Prioritize and Scope—Directs implementers to identify business/mission objectives and high-level organizational priorities. This mission understanding is critical to ensure that resulting risk decisions are prioritized and aligned with stakeholder goals, ensuring effective risk management and optimizing investment.	**Principle 1: Meeting Stakeholder Needs**—Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. An enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific goals and map these to specific processes and practices.
Step 2: Orient—The organization identifies an overall risk approach, considering enterprise people, processes and technology along with external drivers such as regulatory requirements. It identifies threats to, and vulnerabilities of, those assets. **Step 3: Create a Current Profile**—Through use of a Profile template (example provided later in this publication) the organization determines the current state of Category and Subcategory outcomes from the Framework Core (analogous to COBIT 5 governance and management enablers) and how each is currently being achieved.	**Principle 2: Covering the Enterprise End-to-end**—COBIT 5 integrates governance of enterprise IT into enterprise governance: • It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the "IT function," but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. • It considers all IT-related governance and management enablers to be enterprisewide and end-to-end, i.e., inclusive of everything and everyone—internal and external—that is relevant to governance and management of enterprise information and related IT.

Step 4: Conduct a Risk Assessment—The organization, guided by its risk management process, analyzes the operational environment to discern the likelihood of a cybersecurity event and the impact that the event could have. Incorporate emerging risk, threat, and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events. **Step 5: Create a Target Profile**—The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. The organizations may develop additional Categories and Subcategories to account for unique organizational risk. It may also consider influences and requirements of external stakeholders such as sector entities, customers and business partners when creating a Target Profile. **Step 6: Determine, Analyze, and Prioritize Gaps**—The organization compares Current and Target Profiles to determine gaps. It creates a prioritized action plan to address those gaps, drawing on mission drivers, cost/benefit analysis, and risk understanding to achieve the target outcomes. The organization determines the resources necessary to address the gaps.	**Principle 3: Applying a Single, Integrated Framework**—There are many IT-related standards and good practices, each providing guidance on a subset of IT activities. COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT.
Step 7: Implement Action Plan—The organization determines which actions to take in regard to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the CSF identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines and practices, including those that are sector-specific, work best for their needs. An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the Orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the current profile, subsequently comparing the Current Profile to the Target Profile. Organizations may utilize this process to align their cybersecurity program with their desired Implementation Tier.	**Principle 4: Enabling a Holistic Approach**—Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise. The COBIT 5 framework defines seven categories of enablers: 1. Principles, Policies and Frameworks 2. Processes 3. Organizational Structures 4. Culture, Ethics and Behavior 5. Information 6. Services, Infrastructure and Applications 7. People, Skills and Competencies
COBIT 5 Principle 5 is not directly embedded and may represent an opportunity for improvement for the CSF.	**Principle 5: Separating Governance From Management**—The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

Three Lines of Defence

First Line of Defense (Management Controls)

- Administer security procedures, training, and testing
- Maintain secure device configurations, up-to-date software, security patches
- Deploy intrusion detection systems and conduct penetration testing
- Securely configure the network to adequately manage and protect network traffic flow
- Inventory information assets, technology devices, and related software
- Deploy data protection and loss prevention programs with related monitoring
- Restrict least-privilege access roles
- Encrypt data where feasible
- Implement vulnerability management with internal and external scans
- Recruit and retain certified IT, IT risk, and information security talent

Second Line of Defense (Risk Control & Compliance Oversight)

- Design cybersecurity policies, training, and testing
- Conduct cyber risk assessments
- Gather cyber threat intelligence
- Classify data and design least-privilege access roles
- Monitor incidents, key risk indicators, and remediation
- Recruit and retain certified IT risk talent
- Assess relationships with third parties, suppliers, and service providers
- Plan/test business continuity, and participate in disaster recovery exercises and tests

Third Line of Defense (Independent Assurance)

- Provide independent ongoing evaluations of preventive and detective measures related to cybersecurity
- Evaluate IT assets of users with privileged access for standard security configurations, problematic websites, malicious software, and data exfiltration
- Track diligence of remediation
- Conduct cyber risk assessments of service organizations, third parties, and suppliers (note: first and second lines of defense share this ongoing responsibility)

Red Flags Signal Potential Governance Gaps

- Disparate, fragmented governance structure
- Incomplete strategy
- Delays of cybersecurity effort
- Budget cuts and attrition
- Unclear resolve to enforce accountability

Cybersecurity Risk Assessment Framework

Cybersecurity Vulnerabilities, Threats and Risks

Vulnerability	Threat	Risk and Impact
Spear phishing	Attackers may gain access through phish payload or combined social-technical follow-up.	Initial data loss or leakage leading to secondary financial and operational impact
Water holing	Attackers may gain control of attractive websites and subsequent control of visitors.	Initial behavioral errors leading to secondary financial and operational impact
Zero-day	Attacks use zero-day exploits to circumvent existing defenses.	Partial or full control of applications and underlying systems/infrastructure leading to secondary operational impact
Excessive privilege	Inside attacks may happen using inappropriate privileges and access rights.	Full and (technically) legitimate control outside the boundaries of organizational GRC; secondary financial, operational and reputational impacts
Social engineering	Attackers exploit social vulnerabilities to gain access to information and/or systems.	Partial or full control of human target(s), subsequent compromise of IT side; secondary impacts on personal/individual well-being
Extended IT infrastructure advanced persistent threats (APT)	Attacks may target the IT infrastructure underlying critical organizational processes.	Full control of infrastructure, risk of extended control, including public infrastructures or business partners
Vendor/business partner exploit	There are attacks on trusted business partners or vendors, compromising key software or deliverables.	Initial attack through organizational IT directed at third parties, with financial, operational and reputational impact

Source: Adapted from ISACA®, *Transforming Cybersecurity*, USA, 2013. Reprinted with permission.

Cybersecurity Audit Objectives

Cybersecurity Goal	Audit Objective
Emerging risk is reliably identified, appropriately evaluated and adequately treated.	1. Confirm the reliability of the risk identification process.
	2. Assess the risk evaluation process, including tools, methods and techniques used.
	3. Confirm that all risk is treated in line with the evaluation results.
	4. Verify that treatment is adequate or formal risk acceptances exist for untreated risk
Cybersecurity policies, standards and procedures are adequate and effective.	5. Verify that documentation is complete and up to date.
	6. Confirm that formal approval, release and enforcement are in place.
	7. Verify that documentation covers all cybersecurity requirements.
	8. Verify that subsidiary controls cover all provisions made in policies, standards and procedures.
Cybersecurity transformation processes are defined, deployed and measured.	9. Verify the existence and completeness of the transformation process and related guidance.
	10. Verify that the transformation process is implemented and followed by all parts of the enterprise.
	11. Confirm controls, metrics and measurements relating to transformation goals, risk and performance.
Attacks and breaches are identified and treated in a timely and appropriate manner.	12. Confirm monitoring and specific technical attack recognition solutions.
	13. Assess interfaces to security incident management and crisis management processes and plans.
	14. Evaluate the timeliness and adequacy of attack response.

Source: Adapted from ISACA, *Transforming Cybersecurity*, USA, 2013. Reprinted with permission.

AUDIT APP CONTAINER

- Risk analysis and management
- Security awareness and training

- Images
- Registry
- Orchestrator
- Application security during development
- Secure connections
- Hardening
- Container destruction

Audit DEVOPS-CI/CD

10 Important Controls (DevOps Practitioner Considerations –isaca.org)

- Automated software scanning
- Automated vulnerability scanning
- Web application firewall
- Developer application security training
- Software dependency management
- Access and activity logging
- Documented policies and procedures
- Application performance management
- Asset management and inventorying
- Continuous auditing and/or monitoring

Control	Purpose	Implementation	Assessment Criteria
Automated software scanning	A fast release cycle can make it harder to review developed software for security or coding issues. An automated scan during the release process can look for these issues without interrupting the release path	Implement via an automated dynamic or static scanning that triggers as part of the build, testing or release process. Severe issues may warrant further review while lower-priority issues (based on risk tolerance) might be flagged for mitigation in subsequent releases.	• Observe that application code scanning software is in place and kept current as new attacks are discovered. • Examine evidence such as log files to ensure that automated code scans are completed as part of release process.
Automated vulnerability scanning	Tools s.a. Puppet and Chef provide automated configuration anagement functionality. Changes to configuration can impact the security of production platforms. An automated scan as part of the release process can locate those issues without introducing a bottleneck.	Implement via an automated vulnerability assessment that triggers as part of the release process. Severe issues may warrant further review while lower-priority issues (based on risk tolerance) might be flagged for mitigation in subsequent releases.	• Observe that vulnerability assessment software is in place and kept current as new attacks are discovered. • Examine evidence such as log files to ensure that automated vulnerability scans are completed as part of the release process
Web application firewall (WAF) or other layer 7 firewall	In situations where application vulnerabilities occur that cannot be remediated quickly, a WAF or other layer 7 firewall (e.g., extensible markup language (XML) firewall or Java virtual machine (VM) firewall) can provide a stopgap to mitigate the onsequences while the underlying issue is remediated.	Implement via use of an in-line proxy filter (e.g., reverse proxy or web server filter) on the web server or in the communication path.	• Observe network architecture diagrams or other documentation to ensure that a WAF or other layer 7 firewall is in place. • Examine evidence such as log files to ensure that inbound requests are inspected by the WAF or layer 7 firewall.
Developer application security training	Because the path between software development and production is streamlined and automated, training can help developers avoid the inadvertent introduction of vulnerabilities	Train developers on secure coding techniques and commonly occurring application vulnerabilities such as the Open Web Application Security Project (OWASP) Top Ten	• Observe the record of attendance or participation in developer focused application security training. • Observe training materials to ensure that commonly occurring software vulnerability issues are covered. • Perform a periodic review of software to ensure that developers adhere to recommendations such as OWASP recommendations
Software dependency management	Moving to a faster pace of release and automation of build and other intermediate release processes can sometimes make it easier for developers to introduce new dependencies—e.g., new open source or other supporting libraries, new supporting components and middleware or other dependencies	Implementing a process to track these can help offset issues should security or other issues impact supporting components and libraries. Implement tools and/or processes to inventory, track and/or otherwise manage supporting libraries and underlying application components that might be newly introduced.	• Observe that a process is in place to offset unexpected dependencies. • Validate that a record of dependencies exists and newly introduced dependencies can be identified.
Access and activity logging	Separation of duties under DevOps can be fully realized by automated means (in fact, in some cases with more assurance). However, this depends on logging being enabled and logs being retained.	Implement via logging of access and developer activity that results in changes to production code. Logs should contain, at a minimum, the individual responsible for changes and the time that those changes were made.	• Observe log files to ensure that logging is enabled. • For a sample of production changes, observe that the change can be mapped back to specific developers. • Review a sample of historical production changes to ensure that log files are retained
Documented policies and procedures	DevOps processes, while automated and alacritous, should still employ rigor and discipline to ensure that security and risk management goals are met. Having documented policies and procedures describing the release flow is advantageous.	Develop policies and procedures that outline the development and release life cycle. Include policies and procedures in developer training programs.	Review policies to ensure that they exist and cover all aspects of the production release process.
Application performance management (APM)	As development and operations processes become more fluid, it is important that applications continue to perform as expected and remain available to stakeholders.	Application performance management tools can help both provide metrics about application performance and flag potential problem areas when/if they occur. Establish a mechanism for tracking application performance and availability. This can encompass APM specific tools (such as commercial or open source APM products) in conjunction with processes that leverage those tools to collect metrics and drive operations tasks.	• Review operations tools to ensure that application performance and availability issues can be identified. • Review documented processes and procedures to ensure that appropriate personnel are notified or appropriate activities are conducted in light of an issue.
Asset management and inventorying	As DevOps accelerates the development process, consider implementing automated or manual methods to retain a record of applications and important information about them: • Business owner/ purpose • Domain and subject matter experts • Physical or virtual location • Supporting controls and countermeasures	Utilize either an automated tool or manual processes to maintain a record of applications and supporting information about them. Establish tools and/or processes to ensure that this information is kept current and updated.	• Observe tools and/or processes used in support of the application asset management goals to ensure that they are operational. • Review the master inventory for accuracy; e.g., review a sample of applications on the inventory to ensure that entries are accurate and complete.
Continuous auditing and/ or continuous monitoring	Moving to a more real-time and ongoing validation of controls can enable the organization to ensure that controls continue proper operation and that ountermeasures are performing as expected.	Establish a process and supporting tools to continuously validate proper operation of controls.	• Observe mechanisms used to collect information about the control operation. • Validate that coverage is sufficient to address all applications and environments in scope. • Observe a record of data collected to ensure that output is complete and accurate.

Analytics for Internal Audit

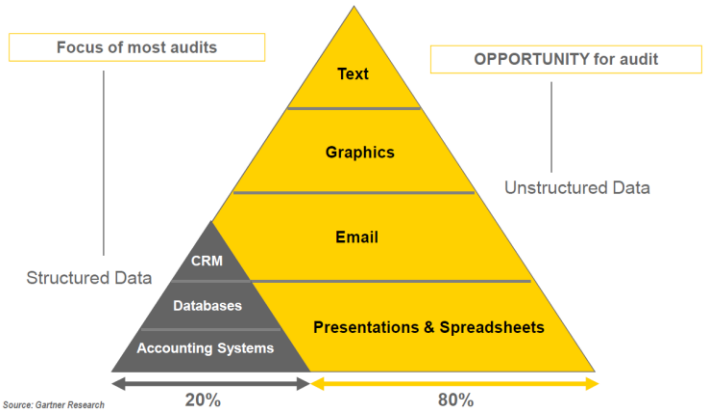
BADIR Framework

PROCESS STEP	DESCRIPTION
Business Questions	Understand what's really going on. Ask the right, relevant questions about the business process. ("6 questions")
Analytical Plan	Goals, Hypotheses, Method/Data Spec, Project Plan
Data Collection	Pull, cleanse, validate (GIGO!)
Insights	Review patterns, prove/disprove hypotheses, present findings in quantified impacts for easy priorities
Recommendations	Based on key insights, supported by detailed findings. Actionable! One Story – Key Message

Common Methodologies

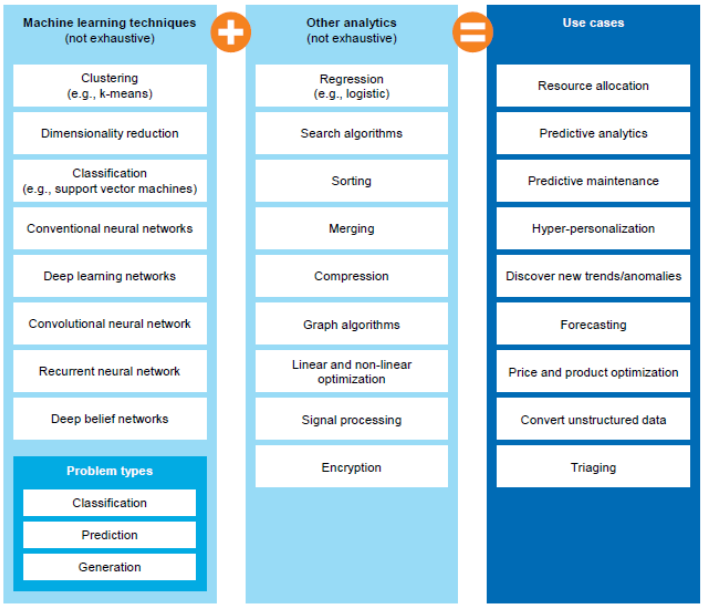
METHOD	DESCRIPTION	USES, EXAMPLES
Aggregate	Describe & compare population(s)/segments	Descriptive, profiling, campaign, winner-loser
Correlation	Relationships between 2 or more factors to explain/drive the other	Pre and post, tests, drivers, dashboards
Trends	Aggregate/correlation over time	Sales, drivers over period of time
Sizing/Estimation	Structured way to estimate w/o history	Business cases depend on external data, assump
Predictive/Time Series	Current & history to predict future events	Drivers of sales conversion, consumer forecasts, other KPI, KRI
Segmentation	Group for meaning	Customization
Customer Life Cycle	Understand buying stages	Sales funnel, progression

Data Source



ML + Analytics Techniques

Machine learning can be combined with other types of analytics to solve a large swath of business problems

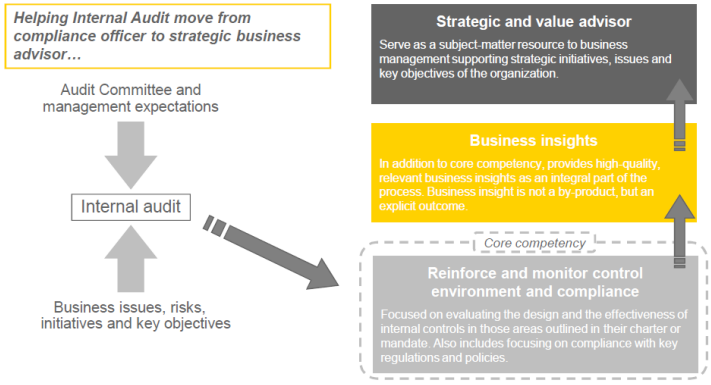


Machine learning can help solve classification, prediction, and generation problems

Classification	Classify/label visual objects	Identify objects, faces in images and video
	Classify/label writing and text	Identify letters, symbols, words in writing sample
	Classify/label audio	Classify and label songs from audio samples
	Cluster, group other data	Segment objects (e.g., customers, product features) into categories, clusters
	Discover associations	Identify that people who watch certain TV shows also read certain books
Prediction	Predict probability of outcomes	Predict the probability that a customer will choose another provider
	Forecast	Trained on historical data, forecast demand for a product
	Value function estimation	Trained on thousands of games played, predict/estimate rewards from actions from future states for dynamic games
Generation	Generate visual objects	Trained on a set of artist's paintings, generate a new painting in the same style
	Generate writing and text	Trained on a historical text, fill in missing parts of a single page
	Generate audio	Generate a new potential recording in the same style/genre
	Generate other data	Trained on certain countries' weather data, fill in missing data points for countries with low data quality

IA Transformation

Helping Internal Audit move from compliance officer to strategic business advisor…



… requires a move beyond core competencies toward skills that elevate its impact.

Audit Opportunities

Audit activity	Example opportunities to use data analytics
Risk assessment	▸ Identify risk assessment priorities by using information gathered from trend analysis, financial ratios and comparisons ▸ Assist with determining scope of audit plan activities (by size/relevance)
Audit planning	▸ Provide a preliminary "scan" of relevant audit information to drive project scope, sampling and fieldwork procedures
Fieldwork procedures	▸ Support testing of controls in an efficient and comprehensive manner ▸ Identify anomalies, trends and potential fraud indicators ▸ Supplement sample testing approaches with full-coverage data analytics
Reporting	▸ Provide quantifiable, fact-based information for reportable issues and exceptions ▸ Supplement reporting with statistical and graphical information gathered during the audit
Monitoring and trending	▸ Automate the ongoing monitoring of the control environment to a sustainable effort through timely exception notification and review ▸ Analyze trends in the company's risk profile and identify opportunities for improvement

#	Audit Area per Internal Audit Plan	Improve Audit Efficiency	Enhance Financial Integrity	Promote Governance, Risk and Compliance	Contribute to Operational Excellence	Improve Cash Flows
1	Purchase to Pay	●	●	●	●	●
2	Order to Cash	●	●	●	●	●
3	Treasury	◐	●	●	◐	●
4	Inventory Management	●	◐	◐	●	●
5	Payroll and Benefits	●	◐	●	◐	◐
6	Fixed Assets	●	◐	◐	●	◐
7	Financial Close	●	●	●	◐	◐

● Higher Potential ◐ Moderate Potential ● Low Potential

Case Study Payroll - Fraud detection case study

Audit Scenario

► A life insurer suspected fraudulent payroll activity. Insurer wanted to assess the payroll information to identify suspicious activity and develop process measures which could be used on a periodic basis as input to business and audit management reports and dashboards.

► The objective was to develop payroll and employee master data analytics initially analyzing the prior two years. Then, implement a periodic retest and reporting process for:

- Employee identification number of deceased individuals
- Employees missing key data points (address, ID, etc.)
- Stratification of payments to employees after termination
- Employees paid not on the EMP master file
- Employees with no or minimal deductions
- Employees hired on irregular days (weekends and holidays)

Results

► Reduced potential exposure to fraud risk

► Reduced erroneous payments and increased cash recovery

- Identified bonus payments incorrectly made to terminated employees
- Eliminated duplicate employees resulting in US$100,000 of payroll over-payments

► Identified process improvement opportunities to reduce fraudulent entries (i.e., ghost employees, payments to terminated employees, etc.)

► Increased management confidence and control through the development of ongoing monitoring reports and management dashboards, including suspicious activities

Case Study Accounts Payable - Process insights case study

Audit Scenario

► E&Y was requested to provide internal audit assistance in providing data analysis testing procedures to facilitate purchasing audits at 15 "in-scope" business units and a centralized accounts payable audit for a $7B medical diagnostics company.

► The objectives of the data analysis testing procedures were to expand the audit coverage by testing full populations and to reduce audit costs by automating manual efforts and reducing the time required in the field. In addition, the procedures aggregate findings in a single view to identify opportunities to enhance the process.

Results

► Pricing consistency – Identified an opportunity to save $3.4M if prices per product were consistent across all business units.

► Missed discounts – Identified over 5k invoices with 10-day or 15-day discount terms that had been paid after the discount period, resulting in $1.3M in lost savings.

► Payments issued to employees set up as vendors – Identified 346 payments that had been issued to vendors with addresses matching an employee's.

► Requisitions created and approved by same person – There were 5 requisitions created and approved by the same person totaling $114K of unauthorized spend.

► As a result of the findings, analytical testing now occurs on a periodic basis for both coverage and audit planning purposes

Case Study Unstructured data analysis case study

Audit Scenario

► A global oil and gas company had large volumes of unstructured data (sales presentations, contracts, competitive advantage material etc) stored on a shared drive. Client was concerned about "what" high-risk data was on the drive, "when" the data was created, and "who" had access to the data

► Objective : perform a business risk assessment to determine what high risk business units use the shared drive and identify the types of high-risk documents stored there. High-risk documents and access controls were analyzed to determine the "who", "what" and "when" around the data to gain a deeper understanding of the chain of communication.

Results

• Identified areas of high-risk information within this shared drive that did not have the appropriate level of controls to protect the sensitive information and other inefficiencies.

► Storage inefficiency- 20% of documents were duplicates (1/2 Word or Excel)

► Unauthorized applications - 36% of the space taken

► Records retention - Documents outside retention policy

► Privacy - Credit card, SS#, bank account information

► Intellectual property - 25% key word hits on "sensitive" terms

Access monitoring analytics

► Segregation of duties assessment

► Key configuration changes

Financial statement computer assisted audit techniques

► Journal entry analytics

► Accounts receivable analytics

Contract audit analytics

► Royalty payment recalculations (incorrect sales figures, royalty rates)

► Invoicing inaccuracies (overpayments, duplicate transactions)

Payment stream analytics (AP, T&E, Procurement Cards)

► Duplicate payments

► Data irregularities and unusual transactions

► Purchasing control violations (split PO's, expenditures above policy limits)

Master file analytics (Vendor, Customer, Employee)

► Missing or unusual information

► Duplicate records

► Conflicts of interest

Unstructured data analytics (i.e., email and text based files)

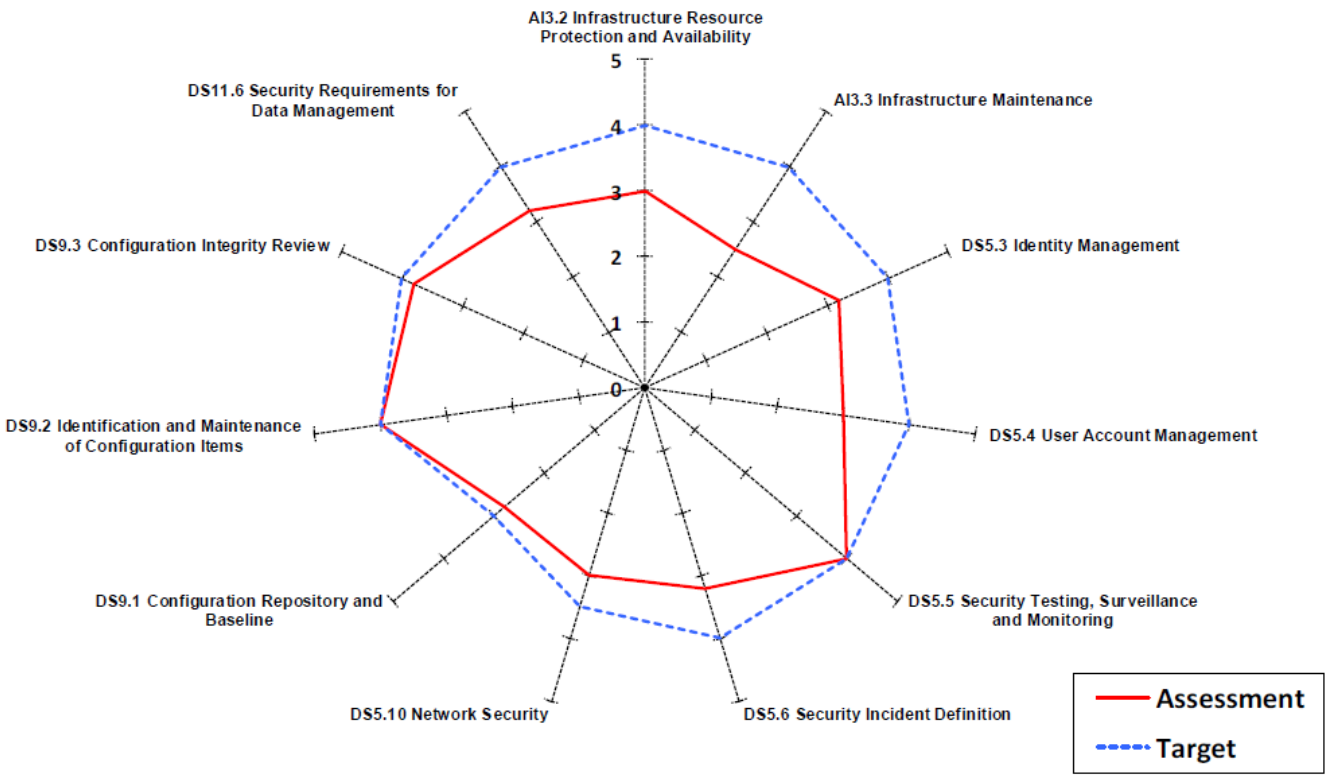
► Recurring content themes and relationship communication patterns

► Contextually valid references to key words or phrases

ISACA AUDIT IF

VIII. Assessment Maturity vs. Target Maturity

This spider graph is an example of the assessment results and maturity target for a specific enterprise.



COBIT

Figure 2—COBIT Process DS5

[A] DS5

Ensure system security.

[B] Information Criteria

- Effectiveness [P]
- Efficiency [S]
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

[C] 11 Control Objectives

5.1 Management of IT security
5.2 IT security plan
5.3 Identity management
5.4 User account managment
5.5 Security testing, surveillance and monitoring
5.6 Security incident definition
5.7 Protection of security technology
5.8 Cryptographic key management
5.9 Malicious software prevention, detection and correction
5.10 Network security
5.11 Exchange of sensitive data

[D] Activities Using a RACI Chart

	CEO	CFO
• Define and maintain an IT security plan.	C	C
• Define, establish and operate an identity (account) management process.	C	C
• Monitor potential and actual security incidents.	A	C
• Periodically review and validate user access rights and privileges.	C	I
• Establish, maintain procedures for maintaining and safeguarding cryptographic keys.	C	I

- Ensure that critical and confidential information is withheld from those who should not have access to it.
- Ensure automated business transactions and information exchanges can be trusted.

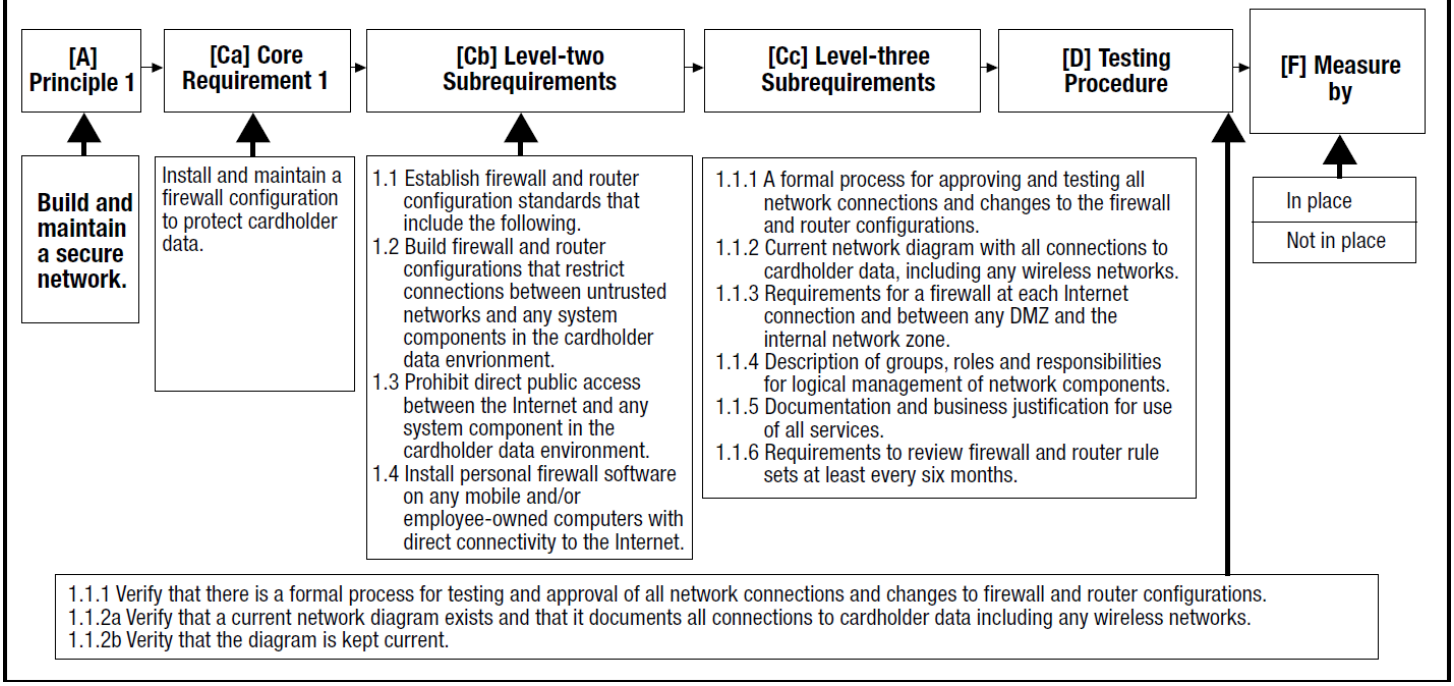
[E] Measured Based on IT Goals

[F] Measured Using Metrics; Assessed Using Maturity Model

- Number of incidents with business impact
- Number of systems where security requirements are not met.
- 0 to 5 levels of customized and COBIT defined

PCI-DSS

Figure 3—PCI DSS Core Requirement 1 of Principle 1



AWS PCI-DSS WORKBOOK

REQUIREMENT	AWS RESPONSIBILITY	CUSTOMER RESPONSIBILITY
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	• All In-Scope Services: AWS maintains instance isolation for host operating systems and the AWS Management Environment including host operating system, hypervisor, firewall configuration, and baseline firewall rules. • AWS meets all requirements for implementing and managing firewalls for the AWS management environment. • Amazon EC2 and Amazon ECS: Amazon VPC Security Groups and network ACLs implement stateful inspection network access control and are suitable for compliant network segmentation	• Amazon EC2 and Amazon ECS: AWS customers are responsible for security group definitions and network access control rules.
Requirement 2: Do not use Supplier-supplied defaults for system passwords and other security parameters.	• All In-Scope Services: AWS develops and maintains configuration and hardening standards for the AWS Management Environment that provides the virtualization technologies and applications for providing cloud services. • AWS maintains configuration and hardening standards for the underlying operating systems and platforms for these services.	• Amazon EC2 and Amazon ECS: AWS customers are responsible for changing default vendor configurations, security controls, and vendor default passwords. • All In-Scope Services: AWS customers are responsible for secure and compliant configuration for all customer-configurable items. This may include OS configuration for Amazon EC2 and Amazon ECS instances, logging and log retention for data base services, or permissions for AWS management functions.
Requirement 3: Protect stored cardholder data.	• All In-Scope Services: AWS Key Management Service (AWS KMS) secures keys using hardware security modules and provides functions to use and manage keys. • AWS CloudHSM secures keys and provides cryptographic functions using customer-dedicated hardware security modules.	• Amazon EC2 and Amazon ECS: AWS customers are responsible for changing default vendor configurations, security controls, and vendor default passwords. • All In-Scope Services: AWS customers are responsible for implementing encryption on all applicable internal and external network connections. (This may require use of AWS optional API encryption). • AWS KMS and AWS CloudHSM: AWS customers are responsible for the creation, usage, and management of encryption keys in accordance with PCI Data Security Standards.
Requirement 4: Encrypt transmission of cardholder data across open, public networks.	• All In-Scope Services: AWS encrypts access and manages encryption within the AWS Management Environment.	• All In-Scope Services: AWS customers are responsible for implementing encryption on all applicable internal and external network connections. (This may require use of AWS optional API encryption).
Requirement 5: Use and regularly update anti-virus software or programs.	• All In-Scope Services: AWS manages anti-virus software for the AWS Management Environment and, where appropriate, for identified services.	• Amazon EC2 and Amazon ECS: AWS customers are responsible for implementing anti-virus software on customer-managed OS instances commonly subject to malware.
Requirement 6: Develop and maintain secure systems and applications.	• All In-Scope Services: AWS maintains security patching, development, and change control of the applications that support the services included in the assessment including web interfaces, APIs, access controls, provisioning, and deployment mechanisms. • AWS develops and manages changes to applications that support the services included in the assessment including web interfaces, APIs, access controls, provisioning, and deployment mechanisms.	• Amazon EC2 and Amazon ECS: AWS customers are responsible for monitoring published OS and application vulnerabilities and patching on instances. • Customers are required to use documented change control for all configurations and customer code.

		• Customers who develop custom code that is used to transmit, process, or store credit card data must comply with requirements for secure development and testing. • AWS Web Application Firewall (AWS WAF): Customers are responsible for protecting their web applications from common web exploits. This includes (but not limited to) configuring access control lists and web application firewall rules for filtering traffic to and from their web applications.
Requirement 7: Restrict access to cardholder data by business need-to- know.	• All In-Scope Services: AWS maintains the access controls related to underlying infrastructure systems and the AWS Management Environment.	• Amazon EC2 and Amazon ECS: AWS customers are responsible for access control within all OS instances. • All In-Scope Services: AWS customers are responsible for configurable access controls within the services such as database users within Amazon RDS. • AWS IAM & AWS Credentials: AWS customers are responsible for managing access to all AWS services that are included in their CDE. AWS IAM can be used to configure resource management and AWS configuration roles and permissions. Customers are responsible for configuring AWS account and session controls to meet PCI requirements. Customers must be aware of AWS guidelines for credentials and access control for AWS resource management.
Requirement 8: Assign a unique ID to each person with computer access.	• All In-Scope Services: AWS provides each user in the AWS Management Environment a unique ID. • AWS provides additional security options that enable AWS customers to further protect their AWS Account and control access: AWS Identity and Access Management (AWS IAM), Multi-Factor Authentication (MFA), and Key Rotation.	• Amazon EC2 and Amazon ECS: AWS customers are responsible for access control within all OS instances. • All In-Scope Services: AWS customers are responsible for configurable access controls within the services such as database users within Amazon RDS. • AWS IAM & AWS Credentials: AWS customers are responsible for managing access to all AWS services that are included in their CDE. AWS IAM can be used to manage resource management and AWS configuration roles and permissions. Customers are responsible for configuring AWS account and session controls to meet requirements. Customers must be aware of AWS guidelines for credentials and access control for AWS resource management.
Requirement 9: Restrict physical access to cardholder data.	• All In-Scope Services: AWS maintains the physical security and media handling controls for the services included in the assessment.	• All In-Scope Services: Any media created outside of the AWS environment is the sole responsibility of the customert
Requirement 10: Track and monitor all access to network resources and cardholder data.	• All In-Scope Services: AWS maintains and monitors audit logs for the AWS Management Environment and AWS service infrastructure.	• Amazon EC2 and Amazon ECS: AWS customers are responsible for logging within all OS instances. • AWS IAM & AWS Console: User activity logs of resource management activities via the console and command line are available to users via Amazon AWS CloudTrail. Amazon AWS CloudTrail must be used to record and monitor AWS resource management activities. • Amazon S3: Users are responsible for configuring bucket logging and monitoring logs. • Amazon RDS & Amazon Redshift: Users are responsible for configuring database access logging and monitoring logs. • Amazon EMR: Customers using Amazon EMR to store cardholder data are responsible for logging access. • Amazon SimpleDB & Amazon DynamoDB: Customers using these databases are responsible for access logging. • AWS Config: Customers using AWS Config to store configuration data and resource inventory are responsible for access logging and monitoring logs. • AWS WAF: Customers using AWS WAF to protect public facing applications including application databases that store cardholder data are responsible for logging access and monitoring logs. • Elastic Load Balancing: Customers using Elastic Load Balancing can monitor applications in real time integrating with Cloud Watch. • All In-Scope Services: AWS customers are responsible for configuration of logging within the services. AWS CloudTrail can be used to log all AWS API calls. • Customers are responsible for monitoring logs for security events. Log monitoring may be implemented with CloudWatch or 3rd party services.
Requirement 11: Regularly test security systems and processes.	• All In-Scope Services: AWS manages rogue wireless access point detection, vulnerability and penetration testing, intrusion detection, and file integrity monitoring for the AWS Management Environment and the identified services. • AWS implements and monitors IDS/IPS on networks that implement AWS services.	• Amazon EC2 and Amazon ECS: AWS customers are responsible for internal and external scanning and penetration testing of their instances and virtual networks. Customers must follow AWS processes for scanning and penetration testing: http://aws.amazon.com/security/penetration-testing/. • AWS customers are responsible for implementing IDS functionality typically using Host-based IDS (HIDS) on network segments they implement and manage.
Requirement 12: Maintain a policy that addresses information security for employees and contractors.	• All In-Scope Services: AWS maintains security policies and procedures, security awareness training, security incident response plan, and human resource processes that align with PCI requirements.	• All In-Scope Services: AWS customers are responsible for all policies and procedures. AWS customers should include AWS as an infrastructure provider for Req. 12.8. Alerts from AWS should be part of the IRP for Req. 12.10.

Requirement A1: Shared hosting providers must protect the cardholder data environment.	• All In-Scope Services: AWS customer instances and data are protected by instance isolation and other security measures in the AWS Management Environment.	• All In-Scope Services: AWS customers may also be considered a shared hosting provider if they run applications or store data for their customers. In this case, customers are responsible for protecting their customer's data within AWS services.
Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	• This appendix concerns on-premise, point-of-sale terminals and is not applicable to AWS. • However, the use of TLSv1.1 and/or v1.2 is required, and AWS fully supports these protocols.	• All In-Scope Services: AWS maintains TLSv1.1 or greater to support customer's PCI workloads. AWS provides a minimum-security policy of TLSv1.0 for customers with non-PCI workloads that still require it. AWS customers are responsible for initiating TLS connections that use TLSv1.1 or greater for PCI compliance.

ON-BOARDING

CIBC Control

CIBC 20 Services (Financial)

AUDIT	Admin of Non-Core loans.
FINANCE	Advertisement Costs
GLOBAP OPS	AR, AP
HR	Business Analysis
LEGAL	Call Centre Supports products for Commercial Banking
MARKETING	Compliance
RETAIL	Fees (Directors, OSFI)
RISK	Financial Analysis
TECH SERV	Financial Ombudsman
WORLD MARKETS	Financial Risk Support
WEALTH	HR - Compensation
	HR - Compliance
	Management Costs
	Project Management
	Resource Centre - reports (M&A, Green sheets, Prospectus') and internet searches
	Stock services
	TI/TS Application Support Cost
	TI/TS Technology Services Cost

CIBC Processes (FCU)

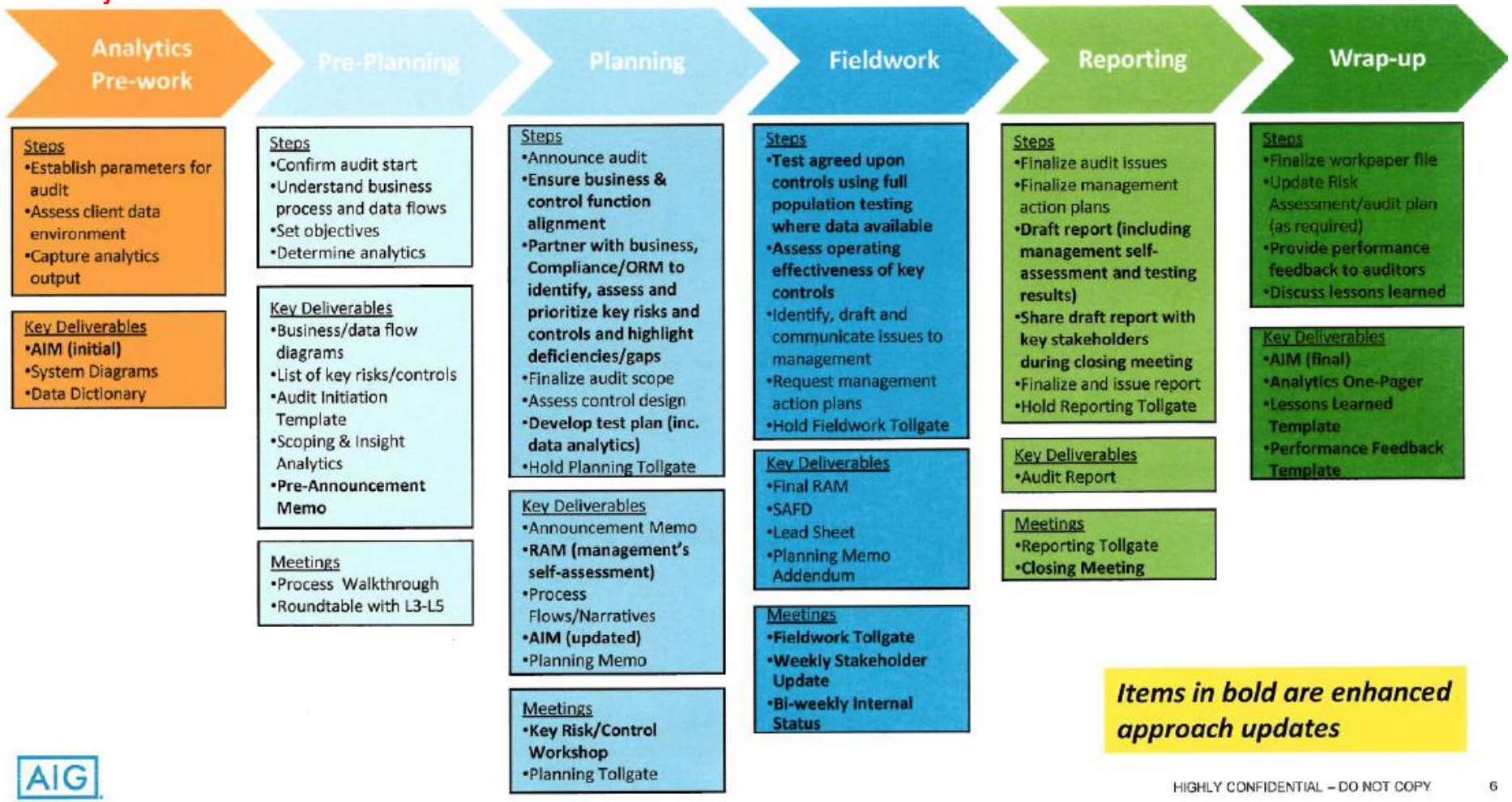
BUSINESS_PROCESS	SUB_PROCESS
A/P	Accrual
Interco loan	Account for loan payable to treasury
Outstanding Cheques Clearing	Accounting Outstanding Cheques
Accrue Liabilities	ID significant individual liabilities
Accrue Obligations related to Securities	Record Repos Position
	Record Securities Sold Short Position
Calculate/ Collect Mortgage Income	Originate a mortgage - recording of acquisition costs on mortgage origination
Income Taxes Note Disclosure	Compilation of Note Disclosure
Note Disclosure Aging of Deposits	Demand, Notice & Term Deposits
Note Disclosure IR Sensitivity	Loans & Deposits Aging & yields
Note Disclosure Mortgage and customer Loans	Mortgages & Consumer Loans
Note Disclosure Segment info	Establish customer CIF (name, address, & permanent information)
Defer Acquisition Cost on Mortgages	Calculate/invoice acquisition cost
	Prepare amortization schedule
Defer Payments to Loblaws	Defer Acquisition Cost of acquiring credit products and points
EUC Applications	General Controls
Financial Statements Preparation	Compilation of Notes to the Financial Statements
Get a mortgage loan on the books	Funding Mortgages
Get the Loans on the books	Attach credit - PLC
	Disburse Funds for Personal Loans
GL/source system balancing	Automatically compare ICBS and GL:M balances
HR	Bi-weekly review of payroll register (Including New Hire, Transfers, and Terminations)
ICBS Application Controls	AS400 Recovery
	Change Management
	ICBS Incident & Problem Management Process
ICBS Information Security	Security Administration
Maintain customer demand (chequing) deposit	Calculate and accrue daily interest
	Maintain interest rates
	Transaction Cheque Clearing
	Transaction processing - EFT
	Transaction processing - POS, ABM, Internet, TB - on Tandem
Maintain customer loan	Maintain interest rates in ICBS
	Recognize interest calc & accrual
	Transaction Processing - Payments or PLC cheques
Maintain customer notice (RSP) deposits	RSP Renewal
Maintain customer notice(savings) deposit	Transaction processing - Internet, ABM, TB (transfers only) - on Tandem
Maintain residential mortgages	All sub-process
	Apply payments to Int. income and principal / Accrue Int. at month-end
	Determine mortgage interest rates
Manage Bank Accounts	Balance & Settle A/P Bank Account
	Balance & Settle ABM Unpostable, All EFT Return Bank Accounts
	Balance & Settle ABM, POS, RB, SCD, Plus, Outbound EFT Bank Accounts
	Balance & Settle Cheque Clearing
	Balance & Settle EFT Bank Account
	Balance & Settle General Operating, Treasury, Mortgage, EFT, USD Bank
	Balance & Settle Guarantee Payments Bank A/C Drafts & MO
	Balance & Settle Guarantee Payments, Cheq Clr Bank A/C Loans
	Balance & Settle Payroll Bank
	Balance & Settle Treasury Bank A/C
Manage Suspense Accounts	Manage Operating Suspense A/C
Other Misc Suspense Accts	Accounting Items in Suspense A/C
Purchase & pay for non interest expenses	Pay Outside Services (Amortized Trailer fees / Commissions)
	Pay Other Misc Expenses
Purchase & pay other expenses	Pay Other Expenses
Recognize deferred taxes	Book Monthly Tax Recovery
	Determine monthly tax rate - Acct
Recognize fee income	Recognize Amicus ABM Surcharge
	Recognize Interac Charges (convenience fee auto charged for each customer txn)
	Recognize Returned Cheque Fees
Recognize FOREX non-trading income	Recognize other income

CIBC 26 Processes (OPC) – 113 Sub-processes

Process	Sub Process
Brokerage & Trade	Broker Services - Cash Processing Broker Services- Collateral Management Cash Management Cash Management - Collection of Foreign Cheques Cash Management-Cheque Issuance Cash Management-Incoming wire payments/Cheque deposits Cash Management-ISI Liasion Desk/Bank Reconciliation-Break Resolution CP Issuance - Billing CP Issuance - Book Based Maturity CP Issuance - Physical Maturity CP Issuance-DCS Settlement CP Issuance-Physical Settlement Domestic Equity /Bonds Settlements Equity Arbitrage Futures & Options Settlements GIC Settlements Institutional Equity Settlements - Equity Arbitrage International Settlements Money Market Money Market DTC/FED Settlements Money Market US Settlements- Physical Trades Over The Counter Receipt of Securities Over The Counter/Branch Receipt of Securities Safekeeping Security Lending and Borrowing Segregation Management Stock Transfers UK Securities Lending
Compliance	COB Disclosure
Credit Mgt	Monitor Credit
Customer Satisfaction	Customer Complaints Management Customer Restitution
Derivatives Settlement Operations	Confirmations Post-Settlement Investigations Pre-Settlement Investigations Settlements
Foreign Exchange	Booking
Maintenance	Account Information Maintenance Customer Information Maintenance Operator Profile Maintenance Suspense Account Maintenance
Manage and Monitor the Imperial vehicles	Execute Transactions Identify Substitute and Replacement Assets Reporting
Management Processes	Investments Lending

	Procedures Information
	Regulatory Compliance
	Sales Management
Origination	Adjudication
	Application Processing
	Funding & Disbursement
Origination (Commercial)	Adjudication (Commercial)
	Funding & Disbursement (Commercial)
Outsourcing	Outsourcing - ADP
Payments Processing	Cash Settlements
	Credit Administration
	Investigations
	Reports Balancing
	Sanction Filtering
	Validation & Message Repair
Portfolio Management	Credit Derivative Hedging
	Credit Derivative Trading
	Establish Portfolio Strategy
	Hedging
	Portfolio Management
Proprietary Products	Account Maintenance (CM, Talvest and SI only)
	Account Opening (PPS)
	Account Opening/Closing/Transfers (CM/Talvest only)
	Client Tax Reporting / Tax filing
	Financial Transactions/ Adjustments
	Trust Accounting
Registered Products	3rd Party Settlements - Brokerage
	3rd Party Settlements-Fixed Term
	Account Transfers (Internal)-Fixed Term
	Adjustments - Brokerage
	Adjustments-Fixed Term
	Client Support-Fixed Term
	Deposits-Fixed Term
	GL Reporting-Fixed Term
	Monitoring & Compliance - Brokerage
	Tax Reporting - Brokerage
	Tax Reporting (GIC Withdrawals)-Fixed Term
	Transfers - Brokerage
	Withdrawals- Brokerage
	Withdrawals-Fixed Term
Sales Fulfillment	Lending - Personal Loan Products
	Lending - Small Business Loan Products
	Small Business Account
Sales Origination	Account Open - Personal Deposits
	Account Open - Small Business Deposits
Security &Control	CSP Application Processing
	Database Control
Service - Inventory Control	Ordering
Servicing	Annual Statement
	Call Center
	Discharge
	Early Renewals
	Product Changes
	Renewals
	Taxes
	Transaction Processing
Servicing (Commercial)	Annual Portfolio Review
	Renewals (Commercial)
	Transaction Processing (Commercial)
Technology Mgt	IT Access Control
3rd Party Mutual Funds	Processing
Trade Finance	Documentation Verification
Transaction Processing	Centralized Instruments Processing
	Cheque Processing
	Deposit Processing
	Inter Branch Payments (IBP) Processing
	Withdrawal Processing

Audit Lifecycle



Items in bold are enhanced approach updates

AIG

STAR AUDIT

Situation	Task	Action	Result
Investments IT Audit 100%	Insourcing 100% in 6 months	- Handover - Priority - Training staff	- Completed 2015 End-of-Year audit - 100% autonomous in 6 months - Confidence from clients, PwC and Internal Audit
Year 2: Increase PwC reliance from 50% to 100%	In addition to ITGC, ITD testing	- Finalize backlog of ITD with PwC and counterpart in Finance - Negotiate test scope, procedures and approach - Define templates, test steps - Get buy-in from business, IT, team	- 89 ITD benchmarked and accepted by PwC in 8 months - 100% turnover in offshore team - 100% changes in ITGC scope - Major IT outsourcing underway
Year 3: Increased application complexity coupled with 100% change in IT Architecture (cloud computing)	In addition to standard Full/False Accept/Reject testing (plain vanilla) code review	- Classify backlog in buckets: "simple"/"complex" - Finalize test procedure for each bucket - Estimate resources - Get buy-in from business, IT and IA management - Train and conduct test	- Underway code review of 50 ltd (including 5 interfaces, 5 Mainframe)

Situation	Task	Failure	Lessons Learned
Year 2: Increase PwC reliance from 50% to 100%	In addition to ITGC, ITD testing	- Get offshore to test 100% ITGC, onshore 100% ITD - High turnover offshore, including 1 star tester - Testing goes into Feb plus onshore reinforcement	- Miscalculate offshore challenges - Did not consult - Did not address the cahllenges as a team
Year 3: Increased testing challenge requires better coordination	- Champion AGILE - Intro 3 weeks SPRINT - Stand-up meeting thrice a week	- Test quality went down => re-work - Pushback from business and IT on 3 weeks SPRINT	- AGILE practices in place (corporate-wide) but not mindset - Seek buy-in (immediate feedback on exceptions => avoid deficiency report - Better embedding of audit into IT - 3-week sprint instead of 3-week deadline => aim for finished product

STAR PROGRAM/PROJECT MANAGEMENT

Situation	Task	Action	Result
Manual work in audit	Automate	- Strategic alignment - ROI - Expected benefits - Urgency/ market reactive - Project type (new, maintenance) - Dependency with major project/program - Risk factor - Time to complete - Complexity	- Benefits communicated and demonstrated - Buy-in from IT, business and management

Situation	Task	Failure	Lessons Learned
Year 2: Huge backlog of tests starting Q3	- Monthly test starting January	Initiative significant change for external customers ⇨ Resistance from IT (supported by business)	- Understand the exact nature of the change for the customers, what they will have to do that is new or different (This refers to CIBC's external customers) - Involve Marketing to create a communication strategy that includes both customers and customer-facing employees - Identify customer- facing employee knowledge/skill gaps and get Training involved to develop an action plan.
Year 3: Increased testing challenge requires better coordination	- Standardize control library	Rationale difficult to understand & communicate New controls too generic/ not correctly reflect the actual controls in-place	Develop a Stakeholder Role Map to identify key audiences affected by the initiative Develop a cascading communication strategy, so that difficult to understand messages can be conveyed face-to-face by the one-up manager Develop feedback mechanisms – Employees Hot Lines, Mailboxes and/or Town Hall Meetings or Workshops designed to convey the messages with time for Q&As