Your Presenter

Gordon Braun

• Managing Director within Protiviti's Kansas City Office
• Member of Protiviti's global IT Effectiveness and Control Team
• 16+ years in information technology, internal audit, and risk consulting spanning a variety of industries, including healthcare, financial services, and consumer products, among other industries
• Experienced in a broad range of projects, from short-term audits and assessments to full-scale process re-engineering and system implementation programs
• ~ At least dozen projects specifically categorized as “IT governance-ish” in the last 5 years
• Gordon.braun@Protiviti.com
• 913.661.7406 - office
About Protiviti

• Protiviti is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services.

• Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

• Protiviti's client base includes over 35% of the Fortune 1000, 35% of the Fortune 500, 40% of the Fortune 100 companies.

• Protiviti is in 20+ countries and has over 70 locations around the world.
Today's Agenda: Critical Questions

- Is IT governance important? Is it a top risk?
- If it is – why do so few companies audit it?
- What are the key elements of IT governance?
- What is Internal Audit's role / responsibility?
- What is involved in a "typical" IT governance audit?
- Can we see some examples and cases?
How important is IT governance?
Is it a top risk?
IT Governance: IT objectives are aligned with business objectives

(we’ll come back to IT governance definitions)
Transformation Within IT Organizations

Protiviti's 2015 IT Priorities Survey confirms that for the second year in a row, IT transformation has become the new normal for companies: Nearly two-thirds of respondents report that some form of “major IT transformation” is underway in their organizations. Even more important: Not only is IT altering its structure, the function is also transforming its fundamental mission. IT’s objective is shifting from leveraging technology in support of the business to the higher-reaching goal of protecting and enhancing business value.

The most notable 2015 priorities for survey participants included:

- **IT Changes with Increased Demand**
- **Collaboration is Key**
- **Security**
- **Search for Balance-Enhance and Protect Value**
- **Strengthening IT Asset and Data management**
IT spend is increasing

<table>
<thead>
<tr>
<th>Worldwide IT Spending Forecast (Billions of U.S. Dollars)</th>
<th>2013</th>
<th>2013 Growth</th>
<th>2014 Spending</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All IT</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td>$669</td>
<td>-1.2%</td>
<td>$697</td>
</tr>
<tr>
<td>Data Center Systems</td>
<td>$140</td>
<td>-0.3%</td>
<td>$143</td>
</tr>
<tr>
<td>Enterprise Software</td>
<td>$300</td>
<td>5.2%</td>
<td>$320</td>
</tr>
<tr>
<td>IT Services</td>
<td>$922</td>
<td>1.8%</td>
<td>$963</td>
</tr>
<tr>
<td>Telecom Services</td>
<td>$1,633</td>
<td>-0.5%</td>
<td>$1,653</td>
</tr>
<tr>
<td><strong>Overall IT</strong></td>
<td>3,663</td>
<td>0.4%</td>
<td>$3,777</td>
</tr>
</tbody>
</table>

| **Core IT**                                             |      |             |                |
| Data Center Systems                                     | $140 | -0.3%       | $143           |
| Enterprise Software                                     | $300 | 5.2%        | $320           |
| IT Services                                             | $922 | 1.8%        | $963           |
| **Total**                                               | $1,362 |             | $1,426         |

*Source: Gartner*
Should you be nervous if your organization is in the 33% of companies that are not going through an IT transformation?
Deploying IT resources to the wrong IT enabled initiatives could result in devastating impacts – agree?
Having a bad process to ensure the alignment of business and IT objectives could be devastating.
Are we auditing the effectiveness of IT governance?
IIA Standard Says Thou Must!

Standard 2110-A2:

The internal audit activity must assess whether information technology governance of the organization sustains and supports the organization's strategies and objectives.
Protiviti IT Audit Benchmarking Survey

Has your IT audit activity completed an evaluation and assessment of your organization’s IT governance process, in accordance with ISACA’s COBIT framework and IIA Standard 2110.A2? (“Yes” responses shown below)

Company Size (Annual Revenue)

<table>
<thead>
<tr>
<th></th>
<th>COBIT</th>
<th>2110.A2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater than US$5 billion</td>
<td>41%</td>
<td>31%</td>
</tr>
<tr>
<td>US$1 billion - US$4.99 billion</td>
<td>34%</td>
<td>29%</td>
</tr>
<tr>
<td>US$100 million - US$999.99 million</td>
<td>43%</td>
<td>28%</td>
</tr>
<tr>
<td>Less than US$100 million</td>
<td>43%</td>
<td>23%</td>
</tr>
</tbody>
</table>
Protiviti IT Audit Benchmarking Survey

If you answered “no” to the previous question, indicate whether you intend to complete an evaluation and assessment of your organization’s IT governance process.

Region

<table>
<thead>
<tr>
<th>Region</th>
<th>Yes, within the next year</th>
<th>Yes, but not within the next year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>COBIT</td>
<td>2110.A2</td>
</tr>
<tr>
<td>Africa</td>
<td>47%</td>
<td>25%</td>
</tr>
<tr>
<td>Asia</td>
<td>30%</td>
<td>18%</td>
</tr>
<tr>
<td>Europe</td>
<td>26%</td>
<td>6%</td>
</tr>
<tr>
<td>Latin America</td>
<td>55%</td>
<td>7%</td>
</tr>
<tr>
<td>Middle East</td>
<td>46%</td>
<td>29%</td>
</tr>
<tr>
<td>North America</td>
<td>24%</td>
<td>12%</td>
</tr>
<tr>
<td>Oceania</td>
<td>17%</td>
<td>8%</td>
</tr>
</tbody>
</table>
Protiviti IT Audit Benchmarking Survey

If you answered “no” to the previous question, indicate whether you intend to complete an evaluation and assessment of your organization’s IT governance process.

**Company Size (Annual Revenue)**

<table>
<thead>
<tr>
<th></th>
<th>Yes, within the next year</th>
<th>Yes, but not within the next year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>COBIT</td>
<td>2110.A2</td>
</tr>
<tr>
<td>Greater than US$5 billion</td>
<td>32%</td>
<td>13%</td>
</tr>
<tr>
<td>US$1 billion - US$4.99 billion</td>
<td>26%</td>
<td>14%</td>
</tr>
<tr>
<td>US$100 million - US$999.99 million</td>
<td>25%</td>
<td>7%</td>
</tr>
<tr>
<td>Less than US$100 million</td>
<td>26%</td>
<td>11%</td>
</tr>
</tbody>
</table>
IT Governance Audit?

• Ensure the IT organization has adopted and applied sound project management techniques for each project undertaken which includes project ownership, user involvement, task breakdown and milestones, allocation of responsibilities, cost, quality plan, and security plan for sensitive systems.

• Verify a change management system exists which provides for analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure. Process should take into consideration the identification of changes, categorization, prioritization and emergency procedures, impact assessment, change authorization, release management, and software distribution.

• Verify that appropriate information security policies have been established and communicated to user community and ensure a process is in place to monitor compliance to security policies.
IT Governance & Business Value

According to Sloan (MIT), entities effective governance can achieve 40% greater returns from IT investment through:

✓ Clarified business strategies and the role of IT
✓ Measurement of IT spend and value
✓ Assignment of accountability
✓ Learning from each implementation to become more adept at sharing and reusing IT assets

According to the IT Governance Institute, fewer than 40% of enterprises feel they have effective IT governance.

*Implies that over 60% of enterprises fail to realize opportunities for enhanced business success & value.*
Why aren’t we auditing IT governance processes, really?
What is IT governance?
IT Governance – an example ISACA graphic
IT Governance – ValIT
IT Governance – Gartner definition

IT governance (ITG) is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.

IT demand governance (ITDG—what IT should work on) is the process by which organizations ensure the effective evaluation, selection, prioritization, and funding of competing IT investments; oversee their implementation; and extract (measurable) business benefits. ITDG is a business investment decision-making and oversight process, and it is a business management responsibility.

IT supply-side governance (ITSG—how IT should do what it does) is concerned with ensuring that the IT organization operates in an effective, efficient and compliant fashion, and it is primarily a CIO responsibility.
The terms "governance", "enterprise governance" and "GEIT" may have different meanings to different individuals and enterprises depending on (amongst others) the organizational context, e.g., maturity, industry and regulatory environment, or the individual context, e.g., job role, education and experience.
CobIT 5.0 – Implementing Governance & Controls

• CobIT 5.0 will provide a renewed and authoritative governance and management framework for enterprise information and related technology

• Builds on the current widely recognized and accepted CobIT framework

• Links and reinforces other major ISACA frameworks and guidance such as Val IT and Risk IT.

• CobIT 5.0 connects to other major frameworks and standards in the marketplace (ITIL, ISO standards, etc.)
IT Governance – CobIT 5

COBIT 5: A BUSINESS FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT
IT Governance – CobIT 5

Figure 2. COBIT 5 Principles

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
IT Governance – CobIT 5

Figure 4. CobIT 5 Goals Cascade Overview

- **Stakeholder Drivers** (Environment, Technology Evolution, …)
  - Influence

- **Stakeholder Needs**
  - Benefits Realisation
  - Risk Optimisation
  - Resource Optimisation

- **Enterprise Goals**
  - Cascade to Appendix D
  - Cascade to Figure 5

- **IT-related Goals**
  - Cascade to Appendix B
  - Cascade to Figure 6

- **Enabler Goals**
  - Cascade to Appendix C
What are the key elements of IT governance?
IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

- IT Governance Institute
Five Elements of IT Governance

**Strategic Alignment**
- Linkage between business and IT plans
- Define IT value proposition / archetype
- Develop IT architecture that enables business objectives

<table>
<thead>
<tr>
<th>IT Governance Practices and Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Strategic Alignment]</td>
</tr>
<tr>
<td>[Risk Management]</td>
</tr>
<tr>
<td>[Performance Management]</td>
</tr>
<tr>
<td>[Resource Management]</td>
</tr>
<tr>
<td>[Value Delivery]</td>
</tr>
</tbody>
</table>

**Risk Management**
- IT risk awareness and understanding risk appetite
- Transparency
- Accountability and risk management processes

**Performance Management**
- Measure strategy implementation
- Measure value delivery
- Drive behaviors and improve

**Resource Management**
- Optimize investment in resources
- Discipline management of resources
- Align capabilities

**Value Delivery**
- Deliver benefits against strategy
- Execute the IT Value Proposition
- Improve intrinsic value of IT

Strategic Alignment

TEN MINUTES LEFT – LET’S DO THE STRATEGY
Strategic Alignment

Objective:
Focus the linkage of business and IT plans; processes to define, maintain and validate the IT value proposition; and on aligning IT operations with enterprise operations.

Example Governance Artifacts:
- IT Strategic Plan
- IT Steering Committee materials
- IT presentations / communications to the Board of Directors
- IT policies and governance processes
- Third Party service provider agreements and RFP process

Typical Control Areas:
- Roles and responsibilities in strategy development (BOD, executive management, IT leadership)
- IT Steering Committee activities
- IT management awareness and participation in the overall business strategy
- Processes to link IT initiatives to one or more of the organization’s strategic objectives
- Communication between IT management and business management and IT management and the Board
- Processes to manage 3rd party service providers
- Impact IT has on the organization – understand the archetype (utility vs. process enabler vs. revenue enabler)
The IT Process Institute (ITPI) identified three common IT alignment archetypes:

1. **Utility Providers**: Are not proactively engaged with the business; primarily focused on "keep the lights on" services.

2. **Process Optimizers**: Are more responsive to business needs; focus on business applications and processes as well as "keep the lights on" services.

3. **Revenue Enablers**: Are well integrated into the business strategy; focus on technology-enabled products as well as business processes and "keep the lights on" services.
“I think, perhaps, we need to come up with a new approach to risk management.”
Risk Management

Objective:
Determine if activities are conducted relating to the identification and analysis of risks impacting the achievement of business objectives and the preparation of financial statements.

Example Governance Artifacts:
• IT risk assessment and risk mitigation strategies and activities
• Communications to executive management and BOD related to IT risk management
• IT risk catalog

Typical Control Areas:
• Alignment of IT risk in ERM programs
• Processes to identify, communicate, and manage IT risks
• Involvement of key stakeholders (business and IT) in risk management strategies
• Risk management activities in key process areas (security, change management, demand management) and projects
• Transparency into the IT risk profile and activities to manage risk (disaster recovery, etc.)
Performance Management
Performance Management

Objective:
Determine if processes exist to ensure IT systems, processes, and personnel are aligned with current and anticipated business needs.

Example Governance Artifacts:
• Performance metrics for services, projects, processes, and systems
• Reports of IT’s performance against defined metrics to key stakeholders and executive management
• Service Level Agreements
• Incident and Problem Management Policies and Procedures
• Cost Allocation Policies and Procedures
• IT Balanced Scorecard

Typical Control Areas:
• Process to define and measure key performance indicators (KPIs)
• Process to review and communicate metrics and KPIs to the business, and update KPIs as the business changes.
• Processes to review key performance metrics and correct items falling below thresholds
• IT scorecard linkage between business goals and IT goals.
• Board of Directors and executive management awareness of IT performance based on quantifiable data
• Budget analysis and benchmarking
• Procurement & sourcing
Resource Management

"As a hypothetical question, Ferguson, if you were being replaced, which one of these people should we hire?"
Resource Management

Objective:
Focuses on the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.

Example Governance Artifacts:
- IT organization chart and job descriptions
- Policies, procedures and processes for resource management
- Sourcing strategy for IT projects
- IT Asset Management policies and procedures
- Architecture policies and standards

Typical Control Areas:
- IT procurement and IT sourcing processes and strategies
- Identification of the resources required to execute IT strategies
- Processes to identify gaps and ensure the availability of IT resources, skills and infrastructure to meet the strategic objectives.
- Processes to forecast future demand for IT resources
- Processes to monitor and manage applications and IT assets
- Processes to assess and implement IT segregation of duties
- IT Architect involvement in strategy development, projects, key decisions, etc.
Value Delivery

What's the ROI of the system you're about to deploy?

It should be in the same ballpark as the system we deployed last year.

In other words, you have not the slightest idea.

Correct!
Value Delivery

Objective:
Evaluate processes to evaluate and approve IT investments; evaluate whether IT delivers the promised benefits against the strategy; understand how IT optimizes costs and improves intrinsic value.

Example Governance Artifacts:
- IT Steering Committee Meeting Minutes
- IT Project Portfolio
- Policies related to identifying, reviewing and approving IT investments
- Business cases for key / large investments
- Processes to assess performance against defined business cases

Typical Controls Areas:
- Linkage between approved IT investments and value to the business
- Relationship between IT project performance indicators and business objectives
- Business case requirements, development and approval process
- Processes to ensure value from IT investments is realized
- ROI for IT investments
- IT demand management and project portfolio management
Assessing IT Governance: Considerations for Internal Audit
IT Governance Assessment: 
**Context & Approach**

IT governance assessment does not need to follow a "one-size-fits-all" audit program approach. When planning a review, the audit team can decide what context is needed to make the audit more impactful.

**Common variations include:**

- ✓ Enterprise-Level Governance
- ✓ Service / Process Area(s) – 5 pillars?
- ✓ Outsourced Service Provider/ Vendor Risk
- ✓ Strategic Initiative(s)
- ✓ Decision-Making & Strategy Alignment

*Budget 2x-3x longer for scoping!*
## IT Governance Assessment: Key Considerations & Resources

<table>
<thead>
<tr>
<th>Strategic Alignment</th>
<th>Risk Management</th>
<th>Resource Management</th>
<th>Performance Measurement</th>
<th>Value Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define IT Value Proposition</td>
<td>Determine Risk Appetite / Tolerance</td>
<td>Optimize IT Resources (e.g., people, technology)</td>
<td>Measure Strategy Implementation</td>
<td>Deliver Against Benefits Strategy &amp; ROI</td>
</tr>
<tr>
<td>Linkage between Business and IT Plans</td>
<td>IT Risk Awareness</td>
<td>Optimize Investment in Resources</td>
<td>Measure Value Delivery to IT Value Proposition</td>
<td>Meeting Business Requirements</td>
</tr>
<tr>
<td>Deliver Value to Products and Services</td>
<td>Transparency</td>
<td>Optimize Knowledge (training, career development)</td>
<td>IT SLAs</td>
<td>Execute the IT Value Proposition</td>
</tr>
<tr>
<td>Increase Managerial Effectiveness</td>
<td>Identify Risk Exposures</td>
<td>Align Capabilities</td>
<td>Operational &amp; Strategic Metrics</td>
<td>On Time / Within Budget</td>
</tr>
<tr>
<td>Assist in Competitive Positioning</td>
<td>Risk Accountability</td>
<td>Co-sourcing / Outsourcing</td>
<td>Reporting</td>
<td>Integrity &amp; Accuracy of Information</td>
</tr>
<tr>
<td></td>
<td>Risk Tracking / Trending</td>
<td>Asset Management</td>
<td>Communication</td>
<td></td>
</tr>
</tbody>
</table>

**COBIT 5**

### Maturity Mapping – IT Governance Model

<table>
<thead>
<tr>
<th>Process Maturity</th>
<th>Strategic Alignment</th>
<th>Risk Management</th>
<th>Resource Management</th>
<th>Performance Management</th>
<th>Value Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial / Ad hoc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repeatable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimized</td>
<td>Key Takeaway: &quot;Optimized&quot; is not an appropriate target for most organizations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- Current State
- Management Goal

**Realization of Value Proposition**

(Example)
Example 1

IT Governance Audit
IT Governance Audit Scope Summary (graphic)

Our findings are organized by the Five elements of IT Governance, as defined by the IT Governance Institute.

- Are we doing the right things?
  - Strategic Alignment
    - Align IT and business
    - Add value to products and services
    - Increase managerial effectiveness
    - Assist in competitive positioning

- Are we getting the benefits?
  - Value Delivery
    - Meeting business requirements
    - On time/ within budget
    - Time to market
    - Integrity and accuracy of information

- How do we compare?
  - Risk Management
    - Determine appetite for risk
    - Determining risk exposures
    - Identifying cost-efficiencies

- Are we effectively managing our assets?
  - Resource Management
    - Optimizing knowledge
    - Optimizing IT resources (i.e., employees, applications, hardware)

- Are we doing them well?
  - Performance Metrics
    - Information Technology ROI
    - Board and executive awareness
    - Operational and strategimetrics

On the right, we use a Capability Maturity Model-based scorecard to indicate where you fall on the continuum.

- Optimized
  - Continuous Improvement – Board is in control of IT strategy; continuously improving governance enterprise-wide; IT activities are directed to business priorities

- Managed
  - Quantitative – IT governance risks managed quantitatively enterprise-wide; IT goals are communicated in business terms and results are reported via balanced scorecard

- Defined
  - Qualitative / Quantitative – the Board has issued guidance and supports IT governance policies, process and standards that are defined and institutionalized

- Repeatable
  - Intuitive – IT governance process is established and repeating; reliance on people continues / IT governance documentation lacking; typically driven by IT management

- Initial
  - Ad Hoc / Chaotic – IT governance is not a priority / unstable environment leads to dependency on herioccs, Senior Management and the Board are only involved in problems
IT Governance Audit Scope Summary (text)

**Background:** Enterprise governance is a set of responsibilities and practices exercised by the board and executive management. The overall objective of enterprise governance over IT is to understand the issues and strategic importance of IT so that the company can sustain its operations and implement strategies required to extend its activities into the future, ensuring that IT’s performance meets the following objectives:
- Alignment with entity objectives and realization of promised benefits
- Use of IT as an enabler by exploiting opportunities and maximizing benefits
- Responsible use of IT resources
- Appropriate management of IT-related risks

**Objectives:** Audit objectives include:
- Determine current state of enterprise governance practices over IT
- Identify enterprise governance practices of IT that are appropriate based on company objectives
- Assess design gaps and improvement opportunities, determining a course of action to achieve appropriate level of enterprise governance over IT

**Approach:** The primary evaluation and assessment will be conducted through:
- Inquiry of key board members, executive management and extended leadership teams to assess current enterprise governance practices over IT in addition to desired practices or expectations.
- Assess current practices and capabilities against an enterprise governance over IT Maturity Model.
- Benchmark (both formally and informally) current company practices.

**Scope:** The following processes are considered to be in scope:
- Strategic Alignment
- Value Delivery
- Resource Management
- Performance Measurement
- Risk Management
IT Governance Audit – Issue Example

Issue #2 – Inconsistent Process for Approving IT-related Projects

**Description**
There is no formally documented process by which IT projects are requested, evaluated, and approved. Some corporate entities and Divisions indicated that they provide business case-related information, but there is no required format to enable consistent review of projects on an equal basis. Additionally, there are no defined criteria by which projects are evaluated to ensure that they are in alignment with the organization’s strategic objectives. Finally, there is no process that validates the achievement of benefits after project completion.

**Quotes**
• “It’s a disjointed process”
• “There doesn’t appear to be an apples to apples comparison between projects”
• “In my opinion, there is no organized process for selecting projects for funding”
• “Within our Division, we have a well-defined process for evaluating and prioritizing projects, but I don’t feel like that’s taken into consideration when IT projects are selected by Corporate”
• “We’re told that certain projects aren’t approved due to lack of funding, but nobody has ever come back to us to ask for additional funds”

**Action Plan Recommendations**
• Agree on key process steps/activities to be carried out, then document and publish those activities.
• Establish formal criteria for project evaluation and a required format for all submitted business cases.
• Modify the project approval process to include feedback regarding project selection/approval.
• Implement a process to review, on a sample basis, completed projects to determine if the stated benefits were realized.
## Issue #4 – Inadequate Performance Metrics and Communication

### Description
The IT organization regularly reports performance metrics to Senior Leadership. However, recipients do not consider the metrics to be reflective of overall IT performance. Additionally, most indicated that positive actions and achievements completed by the CIO organization are not adequately communicated or celebrated.

### Quotes
- “The metrics that we see from IT indicate that everything is great, but I can tell you that based on my organization, that is not the case”
- “They are either measuring the wrong things, or the things they are measuring aren’t being valued correctly”
- “While their metrics may reflect things like ticket closures, what it fails to capture is the fact that people do anything they can to not call the service desk due to the frustrations that they experience”
- “IT doesn’t celebrate their achievements - when they increased the VPN capacity, which was a great thing for the organization, it wasn’t communicated at all”

### Action Plan Recommendations
- Solicit feedback from Corporate functions and departments to establish new metrics that would be more useful or representative of the value of the services they receive.
- Evaluate the existing metrics reported by IT and determine if there are either additional data points that can be communicated, or changes to existing data points which would more accurately portray level of service.
- Implement a mechanism to communicate IT achievements to the organization (i.e. – email, intranet notice, etc.)
## IT Governance Audit Results – CMM Summary

<table>
<thead>
<tr>
<th>Process Maturity</th>
<th>Realization of Value Proposition</th>
<th>Risk of Failure</th>
<th>Initial / Ad hoc</th>
<th>Repeatable</th>
<th>Defined</th>
<th>Managed</th>
<th>Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Legend:
- Current Assessment Status
- Desired Status

#### Strategic Alignment
- IT is integral to business achieving strategic objectives. IT presents solutions to the business in a proactive manner. The board is engaged and proactive.

#### Value Delivery
- IT is viewed as a strategic partner of the business. Solutions are presented to the business - then are delivered on time/budget/ scope.

#### Risk Management
- Risk management is a continuous process coordinated by the board and management. Organization risk tolerance is well known.

#### Resource Management
- Resources are deployed strategically considering internal and external models using defined evaluation criteria based on strategic objectives.

#### Performance Metrics
- A balanced scorecard is utilized to monitor IT effectiveness. The scorecard is presented to the board and other key executives for critical evaluation and response.

#### Process Maturity
- Optimized
  - The board or executive management evaluates business strategy to ensure alignment on a regular basis. Long term, tactical IT plans map to business strategy.

- Managed
  - A formal process to evaluate and prioritize potential IT projects is defined; established criteria are consistently applied to facilitate cross-functional committee decisions.

- Defined
  - IT maintains existing systems, but is viewed primarily as an order taker. Project decisions involve business personnel and require business case format.

- Repeatable
  - IT projects and services may or may not align with business needs or objectives. Project decisions are made unilaterally or without established criteria.

- Initial / Ad hoc
  - Inherently ineffective communications between IT and the business. Projects are often delayed, do not deliver expected scope, or are over budget.
**IT Governance Audit Results – 5 Pillars Example**

<table>
<thead>
<tr>
<th>Optimized</th>
<th>IT is viewed as a strategic partner of the business. Solutions are presented to the business - then are delivered on time/ budget/ scope.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed</td>
<td>IT is cost-effective in delivering high-value services that meet the needs of the enterprise. Communication is frequent and structured; IT proactively seeks to enhance business value.</td>
</tr>
<tr>
<td>Defined</td>
<td>IT is viewed as an enabler of business processes and there are activities in place that confirm that business requirements are being met and budget goals are achieved.</td>
</tr>
<tr>
<td>Repeatable</td>
<td>Business views IT as a utility. There are consistent communications between the groups, but IT generally is contacted when there are issues.</td>
</tr>
<tr>
<td>Initial / Ad hoc</td>
<td>Irregular or ineffective communications between IT and the business. Projects are often delayed, do not deliver expected scope, or are over budget.</td>
</tr>
</tbody>
</table>

---

**Legend:**
- Current Assessment Status
- Immediate Goal (1 - 2 years)

**Observations for Current State**
- The business views IT primarily as a “utility” as opposed to a “process enabler.” Most know how IT is doing only when problems arise or when projects are not going well.
- Senior leadership would like to improve the value IT provides to the organization beyond that of a utility, primarily through improving alignment of business and technology objectives.
- Business and IT leadership have a shared responsibility to jointly agree upon and establish high level priorities to best align IT resources with business strategy. Current governance practices have resulted in sub-optimal results and mutual dissatisfaction.
- There is a perception of failed projects over time that has put a stress on relationships between the business and IT; confidence in IT and a culture that sees IT as a key enabler of their needs will take time to develop.
- There is no consistent mechanism in place to assess the value of projects that are being considered for funding (i.e., a business case template) or for validating that identified benefits are achieved after projects are completed.

**Recommendations and Next Steps**
- Define a process to manage the consideration and approval of IT projects on an ongoing basis. The IT steering committee will own this process and require adherence to all projects that will receive IT resources.
- Develop a business case template that will be completed for all IT projects to be considered for certain levels of funding -- the business case should include hard and soft benefits for management’s consideration. Define and publish criteria by which business cases will be evaluated; criteria should tie to corporate objectives.
- The project approval process should link to the overall IT demand management function so that smaller efforts and maintenance items are considered as project scheduling is completed.
- The project approval process should be communicated to an appropriate level of management so there is an understanding of how IT resources are requested, evaluated, and approved.
- Create greater transparency of IT activities by reporting the status of all projects that are underway to the IT steering committee on a regular basis; project status should be reported for all projects, not just the projects that are behind or off schedule.
Example 2

Benefits Realization Review
Benefits Realization Review Scope

• As a part of the annual budget allocation and project approval activities, each potential IT initiative is required to submit a benefits baseline for each Business Case (BC). The project sponsor, with CIO’s guidance, commits to and is accountable for tracking, delivery and realization of benefits.

• Internal Audit reviewed the benefits realization process and performed an assessment to determine whether the “direct and measurable” benefits contained in the business case were realized as stated. Other “soft” benefits, such as improved employee satisfaction, were not considered.

• Internal Audit did not review any of the costs that were incurred to fund the achievement of benefits, nor was the overall ROI considered.

• It was the responsibility of the initiative team to provide evidence substantiating the benefits attained.
Benefits Realization Review Results

- The Business Travel Services: SBT business case identifies 4 key benefits, among others:
  - Lower transaction fees of $1M over a three-year period.
  - Availability of 24 by 7 services through an online booking tool will reduce traveler reliance on higher-cost after-hours "emergency" services, as well as provide an official company-sponsored alternative to booking online directly through the Internet.
  - Use of self-booking tools facilitates enhanced policy compliance through visible display of cost-effective travel options and the ability to include compliance messaging at the user's point-of-need. In addition, certain out-of-policy options (e.g. higher fare class) can be blocked with the online tool, if required.
  - Based on the industry average reduced ticket price outside North America of 8-15%, we have projected a conservative 10% lower average lower ticket price in each of the major markets. The result is savings of $2.1M over a three-year period.
- The business case indicates that $330,619 of “direct and measurable” benefits will be achieved in FYxx. The initiative team submitted an FYxx benefits realization claim of $727,844.

<table>
<thead>
<tr>
<th>Benefit Type</th>
<th>Organization Accruing Benefit</th>
<th>Benefit Operating Function</th>
<th>Benefit Begins FQ/FYYY</th>
<th>FY20xx</th>
<th>FY20xx Benefits Claim</th>
<th>FY20xx</th>
<th>FY20xx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct &amp; Measurable</td>
<td>XYZ</td>
<td>Business Process Operations</td>
<td>FQ1/20xx</td>
<td>$330,619</td>
<td>$727,844</td>
<td>$1,068,709</td>
<td>$1,662,156</td>
</tr>
</tbody>
</table>
Evidence that benefits were realized

- Corporate Travel contract agreement indicates a blended, agent assisted transaction price of $30 per transaction vs. an online transaction price of $10 per transaction. Datasource reports indicate total number of transactions by category resulting in savings of $239,921.

- Datasource reports also indicate gross savings based on average ticket price by market resulting in savings of $487,923.

- Additional detail only available in FYxx reporting indicates a model of savings for international and domestic ticket types that substantiate the claimed 2% savings on average ticket price for FY04.

Conclusion

- While the business case indicates $330,619 of benefits would be attained in FYxx, initiative management was able to substantiate the benefits realization claim of $727,844 of reduced transaction fees and ATP.

<table>
<thead>
<tr>
<th>Benefit Type</th>
<th>Organization Accruing Benefit</th>
<th>Benefit Operating Function</th>
<th>Benefit Begins FQ/FYYY</th>
<th>FY20xx (Planned)</th>
<th>FYxx Actual Benefits</th>
<th>Actual Benefits vs. Planned</th>
<th>FY20xx (Planned)</th>
<th>FY20xx (Planned)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct &amp; Measurable</td>
<td>XYZ</td>
<td>Business Process Operations</td>
<td>FQ1/20xx</td>
<td>$330,619</td>
<td>$727,844</td>
<td>$397,225</td>
<td>$1,068,709</td>
<td>$1,662,156</td>
</tr>
</tbody>
</table>
Example 3

Performance Measurement - Projects
# Project Tracking – bad example

<table>
<thead>
<tr>
<th>PROJID</th>
<th>TITLE</th>
<th>PROJ OWNER</th>
<th>ITHRSLOGGED</th>
<th>USERHRSLOGGED</th>
<th>LIFETIMEACTUAL</th>
<th>STATUS</th>
<th>ACTUALENDDATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>86</td>
<td>New website</td>
<td>Joe</td>
<td>13835</td>
<td>95</td>
<td>13930</td>
<td>In Progress</td>
<td>2012-12-11</td>
</tr>
<tr>
<td>88</td>
<td>(UL and Trad) for internal</td>
<td>Bob</td>
<td>11123</td>
<td>48</td>
<td>11171</td>
<td>In Progress</td>
<td>2014-05-27</td>
</tr>
<tr>
<td>209</td>
<td>XYZ version 17 upgrade - Dev</td>
<td>Tom</td>
<td>2960</td>
<td>261</td>
<td>3221</td>
<td>Complete</td>
<td>2012-12-11</td>
</tr>
<tr>
<td>160</td>
<td>New Site for existing products</td>
<td>Kirstin</td>
<td>2953</td>
<td>0</td>
<td>2953</td>
<td>Not Started</td>
<td>2012-12-11</td>
</tr>
<tr>
<td>89</td>
<td>Electronic contracting)</td>
<td>Greta</td>
<td>2413</td>
<td>235</td>
<td>2648</td>
<td>Complete</td>
<td>2013-12-13</td>
</tr>
<tr>
<td>386</td>
<td>LongView (Internal Resources)</td>
<td>Bill</td>
<td>1571</td>
<td>0</td>
<td>1571</td>
<td>In Progress</td>
<td>2013-12-13</td>
</tr>
<tr>
<td>130</td>
<td>ABC software upgrade)</td>
<td>Joey</td>
<td>1225</td>
<td>110</td>
<td>1335</td>
<td>Complete</td>
<td>2013-03-25</td>
</tr>
<tr>
<td>94</td>
<td>CRM system</td>
<td>Tom</td>
<td>1185</td>
<td>0</td>
<td>1185</td>
<td>Complete</td>
<td>2013-03-25</td>
</tr>
<tr>
<td>163</td>
<td>2011 - Communication App</td>
<td>Ralph</td>
<td>1111</td>
<td>0</td>
<td>1111</td>
<td>Cancelled</td>
<td>2013-03-25</td>
</tr>
</tbody>
</table>
Project Governance – good example

### Summary Data

<table>
<thead>
<tr>
<th>Bus Sponsor</th>
<th>IT Sponsor</th>
<th>Portfolio Director</th>
<th>Project Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>K. Johnson</td>
<td>H. Stevens</td>
<td>D. Johnston</td>
<td>P. Kellner</td>
</tr>
</tbody>
</table>

**Start Date** | **End Date** | **State**
---|---|---
Jan 20xx | Oct 20xx | Execution

### Status Summary

<table>
<thead>
<tr>
<th>Status Date</th>
<th>Overall Status</th>
<th>Schedule</th>
<th>Cost</th>
<th>Benefit</th>
<th>Issues/Risks</th>
<th>% Complete</th>
<th>% Time Elapsed</th>
<th>% Spent (of total bid)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/10</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>Y</td>
<td>79%</td>
<td>91%</td>
<td>68%</td>
</tr>
<tr>
<td>10/10</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>G</td>
<td>81%</td>
<td>78%</td>
<td>68%</td>
</tr>
</tbody>
</table>

1 End date extended to Q3 20xx from Q2, to accommodate approved roadmap change.
2 % Time Elapsed recalculated to align with approved roadmap change. Extends project to Q3 20xx.
3 % Spent recalculated to align with $150K allotted to project in October 20xx for other work.

### Schedule

- Settlement Options/Detail statements on Client Quarterly Review - launched
- Brokerage data on ABC - targeted launch
- Fixed annuity detail statements - targeted launch
- Mutual fund detail statements, risk product summary data, bank data and Client Choice summary data on targeted launch
- Detail statements co-mingled with launch

**Progress to date**

- Status Date: 10/31/20xx
- Milestone

### Cost Summary

<table>
<thead>
<tr>
<th></th>
<th>Total Budget</th>
<th>Total Released by FEC</th>
<th>Planned Spend To-date (P)</th>
<th>Actual Spend To-date (A)</th>
<th>Spend to Date Variance (A-P)</th>
<th>20xx Allocation</th>
<th>20xx Forecast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>$2.5M</td>
<td>$1.5M</td>
<td>$1.6M</td>
<td>$1.8M</td>
<td>$0.2M</td>
<td>$0.6M</td>
<td>$0.9M</td>
</tr>
<tr>
<td>External (Surplus)</td>
<td>$5.2M</td>
<td>$4.3M</td>
<td>$3.9M</td>
<td>$3.5M</td>
<td>$(0.4M)</td>
<td>$1.5M</td>
<td>$1.3M</td>
</tr>
<tr>
<td>Totals</td>
<td>$7.7M</td>
<td>$5.8M</td>
<td>$5.5M</td>
<td>$5.3M</td>
<td>$(0.2M)</td>
<td>$2.1M</td>
<td>$2.2M</td>
</tr>
</tbody>
</table>

### Issues / Risks

- Resource constraints exist for adding brokerage information to Statements. Team pursuing solution with resource management.

### Targeted Business Benefits to be Delivered

- Meet members needs thereby increasing member satisfaction & net promoter scores. This will be achieved by:
  - Providing members with clear and easy to understand information on the performance of their investment products purchased through Client
  - Reducing paper mailed to members
  - Increasing member access options through e-delivery
  - Enhancing the overall impression and branding of Client as a competent financial services provider that provides high quality statements to its members
  - Provide Field Representatives with improved tools for tracking members’ product holdings and performance.

### Progress / Highlights / Next Steps

- Preferred House-Holding: Targeted to launch Q4 20xx.
- Brokerage summary information: Targeted to launch Q1 20xx.
- Fixed annuity detail statements: Targeted to launch Q1 20xx.
- Mutual fund detail statements, risk product summary data, bank data and Client Choice summary data: Targeted to launch Q2 20xx.
- Variable Universal Life (VUL) statements co-mingled with TQR: Targeted to launch Q3 20xx.
Case Study – Real Life
Case Background

• Franchisor - 700 + franchises around the world; approaching $1bn in global franchise revenue

• Technology Project: Replacement of core operational software

• Legacy software was Access-based – single instances across all franchises – data is loaded back to corporate for consolidation and reporting

• Decision was made to purchase packaged software and heavily customize it; project cost was over $20m

• IT Steering Committee comprised of dedicated and smart people was setup and the entire organization was behind the project

• A PMO of existing employees was established and some elements of project management were available for consideration

• We were engaged by the President, who knew something was starting to smell bad

• “Bury the auditor” technique was deployed - - but the issues were numerous
## Case 1 - Review Findings

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Related Observations</th>
<th>Benefits of Implementation</th>
<th>Challenges For Implementation</th>
<th>Time Impact</th>
<th>Cost Impact</th>
<th>People Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Develop a defined scope and roadmap for all NANS-related initiatives. This document should include the prioritization of each project, clear milestones that allow for the tracking of progress, and high-level estimates of completion dates for additional functionality.</td>
<td>1. There is no clear overall strategy and vision for NANS that has been communicated to the SLT and franchise owners. 2. Key project-related documents such as a project plan and estimated timelines have not been created and communicated to management and the network. 3. Confusion exists regarding the scope of NANS and when specific functionality will be available. 4. The implementation timeline of reaching a “tipping point” by the end of 2014 seems lengthy, given the amount of resources currently devoted to the NANS project. 5. Budgets and timelines are consistently missed causing a lack of confidence in the implementation.</td>
<td>- Clear alignment of business goals with IT goals. - Decreased confusion regarding expectations for NANS. - Increased visibility and transparency to the NANS project. - Increased feeling of accountability for key project managers and sponsors.</td>
<td>- Due to the current resource requirements of the project, it may be difficult to engage the necessary people to develop the roadmap. - There is the potential for Franchise Owner dissatisfaction depending on how key functionality is prioritized and how quickly it is delivered.</td>
<td>Medium</td>
<td>Low $</td>
<td>High ▲▲▲</td>
</tr>
</tbody>
</table>
### Case 1 - Review Findings

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Related Observations</th>
<th>Benefits of Implementation</th>
<th>Challenges For Implementation</th>
<th>Time Impact</th>
<th>Cost Impact</th>
<th>People Impact</th>
</tr>
</thead>
</table>
| **B.** | Identify the individual(s) ultimately responsible for the NANS project.  
- This individual should be involved in all key project-related decisions, including budget and timeline considerations.  
- More emphasis should be put on the NANS Steering Committee to ensure they are also included in major project decisions.  
- While the overall NANS owner should come from the business, there should be an individual who manages the project solely from a technology perspective, working closely with the project owner. | 1. It is not clear who is the ultimate owner of the NANS project.  
- There are individuals within the organization that view Technology as the overall NANS owner, while others see the owner as being various members of the SLT.  
2. Although a steering committee has been established for the NANS project, there has not been consistent attendance and participation during bi-weekly committee meetings.  
3. A full understanding of all project costs, including estimate to complete, has not been developed or communicated to the SLT. | - Clear ownership will increase accountability for the project.  
- Active participation from the steering committee will help ensure project objectives and targets are achieved. | Medium | Low $ | Medium ▲▲ |
10 Takeaways!

1. We are in a period of extraordinary technology development and change – don’t put your head in the sand.

2. There is no one definition of IT governance, but effective governance will ultimately lead to better performance. It is critical!

3. Internal Audit should have a view whether IT governance of the organization sustains and supports the organization's strategies and objectives.

4. When assessing IT governance, it is important to leverage research, frameworks, and other best practice tools as "audit accelerators."

5. IT governance audits require an effective IT audit function and will raise the profile of IT audit significantly.
10 Takeaways!

6. There are multiple IT governance assessment approaches. Auditors should consider the changing needs of the enterprise when planning IT governance assessments.

7. An IT governance audit can be a very effective way to build a relationship with IT leadership.

8. Remember to budget 2-3x longer for scoping when planning for an IT governance project.

9. Adding additional time to the reporting process is also a very good idea – socializing the issues and obtaining buy in can take some time.

10. If your IT audit scope/ risk assessment results haven’t changed in the last few years, you likely have a problem (an IT problem, or an IT audit problem).
Confidentiality Statement and Restriction for Use

This document contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly-owned subsidiary of Robert Half International Inc. ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public, should be used solely and exclusively to evaluate the capabilities of Protiviti to provide assistance to your Company, and should not be used in any inappropriate manner or in violation of applicable securities laws. The contents are intended for the use of your Company and may not be distributed to third parties.