Questions from the CEO

Do possible external environment changes threaten achievement of my company's strategy objectives?

Could assets of my company be stolen?

Are factors that might impair my business processes within reasonable limits?

Do internal processes and reports provide adequate measurement of threats to assets, processes, and strategy achievement?

Are my reports to outsiders in compliance with applicable standards, laws, and regulations?
Risk Definition

The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

Then you determine the impact

Risk Assessment

Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard).

Quantitative risk assessment requires calculations of two components of risk: $R$, the magnitude of the potential loss $L$, and the probability $p$, that the loss will occur.

From Wikipedia, the free encyclopedia
Risk Management

Understanding all the possible things that might happen.

Estimating the consequences of those events and situations, how they might affect company's ability to achieve its objectives and the likelihood of those effects.

Determining whether those consequences are acceptable/desirable.

Taking action to modify the consequences and/or their likelihood.

Risk Management

The management of risk is not left to a periodic meeting, analysis, or review of a report. It is an integral part of every decision, from setting corporate strategies, to reviewing and assessing performance.

Reviewing a list of top risks is a periodic exercise at best. The business is making "small" decisions that could have a huge impact on the enterprise as a whole. It is something that every executive, manager, and decision-maker practices every minute of every day.

Risk is managed effectively when you can influence the making of decisions such that the right level of the right risks is being taken.
IT Risk Assessment (RA)

- IT Organization

- Projects

The Bigger Picture

ERM: process applied across all levels of an enterprise designed to identify, prioritize and respond to risks to provide reasonable assurance of the achievement of enterprise objectives.

IT: application of the ERM process to IT as the enterprise. Not limited to technology risks – looks at all risks that could affect IT’s ability to achieve its objectives which are tied to the enterprise objectives.
The Need for RA

- Business world is constantly changing
- Increased regulatory requirements:
  - Sox, MAR, Basel, Anti-Money Laundering (AML)
  - Information privacy
- Greater IT exposure / risk of loss
- Shareholders want to know if companies have the correct controls in place
- New systems development

The Need for RA

- Dependence on Internet, telecommunications, mobile processing, PSD, PCI, etc.
- Connectivity ... VPNs and Internet with Suppliers, Customers, Providers
- More and smarter hackers with better tools
- Corporate espionage
- Information terrorism
Frequency

- Annually
  - January
  - December
- Monthly
- Daily
- Continuously

Drivers of RA

IIA / ISACA
NIST 800-30, 800-39
COSO

Risk Assessment
Guiding Principles of Risk IT

- Always connect to enterprise objectives.
- Align the management of IT-related business risk with overall enterprise risk management.
- Balance the costs and benefits of managing risk.
- Promote fair and open communication of IT risk.
- Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels.
- Understand that this is a continuous process and an important part of daily activities.
Risk IT Three Domains

Risk Governance Essentials:
- Responsibility and accountability for risk
- Risk appetite and tolerance
- Awareness and communication
- Risk culture

Risk Evaluation Essentials:
- Risk scenarios
- Business impact descriptions

Risk Response Essentials:
- Key risk indicators (KRI)
- Risk response definition and prioritization
Current Executive Priorities for IT

**CEO/CFO**
- Increase the value received from IT
- Make sure IT is supporting the business strategy
- Measure and manage IT appropriately
- Spend the appropriate amount of money on IT
- Have the skill sets and experience needed in IT
- Reap business benefits from recent regulatory compliance changes

**Senior Business Leaders**
- Use IT to improve the business
- Develop a common language for communicating with IT
- Make IT a part of the team
- Deliver IT projects on-time and on-budget, along with the expected results

**Senior IT Leaders**
- Demonstrate the value IT provides to the business
- Secure the resources IT needs to deliver results
- Have a place at the executive table and a common language for communicating with the business leaders
- Achieve excellence in all aspects of IT operations

Domains of COBIT 5

- **Align, Plan and Organize**
- **Build, Acquire and Implement**
- **Deliver, Service and Support**
- **Monitor, Evaluate and Assess**
COBIT

**Align, Plan, Organize**

<table>
<thead>
<tr>
<th>APO 03</th>
<th>Manage Enterprise Architecture</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO 04</td>
<td>Manage Innovation</td>
<td>Management</td>
</tr>
<tr>
<td>APO 05</td>
<td>Manage Portfolio</td>
<td>Management</td>
</tr>
<tr>
<td>APO 06</td>
<td>Manage Budget and Costs</td>
<td>Management</td>
</tr>
<tr>
<td>APO 07</td>
<td>Manage Human Resources</td>
<td>Management</td>
</tr>
<tr>
<td>APO 08</td>
<td>Manage Relationships</td>
<td>Management</td>
</tr>
<tr>
<td>APO 09</td>
<td>Manage Service Agreements</td>
<td>Management</td>
</tr>
<tr>
<td>APO 10</td>
<td>Manage Suppliers</td>
<td>Management</td>
</tr>
<tr>
<td>APO 11</td>
<td>Manage Quality</td>
<td>Management</td>
</tr>
<tr>
<td>APO 12</td>
<td>Manage Risk</td>
<td>Management</td>
</tr>
</tbody>
</table>

**IT Risk Management (ITRM) Framework**

IT Risk Management process begins with the development of the IT Risk Management Framework.

IT Risk Management is aligned with the Enterprise Risk Management domains.

**Principal Stakeholders**
- CISO
- Board of Directors
- ITRM Steering Committee

**Enterprise Risk Management Domains**
- Finance to Board of Directors
- COBIT Control Objectives

**ITRM Major Activities / Processes**
- COBIT Control Objectives
ITRM Responsibilities

• Perform analysis on risk assessments conducted throughout IT and business units. A partial list includes:
  • Regulatory Assessments
  • Security Risk Assessments
  • Internal Control Testing
  • Disaster Recovery Tests
  • HIPAA Risk Assessments
  • External Risk Assessments (i.e. Gartner)

• Analyze each risk using the IT Risk Context and provides a risk score using the normalized risk scoring structure
  • The Normalized Score combines qualitative assessment of Impact and Likelihood with quantitative scoring to produce a score of 0 to 100

• Evaluate and determine if appropriate responses or recommendations have been provided

Risk Reporting & Metrics

• The final step is the development of reporting and metrics for senior leadership.
• IT Risk Management provides sufficient reporting capability in order to assist leadership in making risk aware decisions.
## IT Risks

- Use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

- Contribution of IT to new or improved business solutions, usually in the form of projects and programs.

- (Missed) opportunities to use technology to improve efficiency or effectiveness of business processes, or as an enabler for new business initiatives.

- The performance and availability of IT services.

## Business Risks

- Inability to deliver services/products efficiently and effectively and comply with regulations or contractual obligations.

- Lack of access controls → fraud risk, disclosure.

- System does not meet the user needs.

- Poor system performance/throughput impacts user productivity.

- Data integrity problems.

- Users frustrated with reporting capabilities … develop their own using Excel spreadsheets.

- Users not adequately trained and do not know how to properly use the system.
Business Impact

Business needs an effective identification and assessment of business risks associated with IT, where the risks are greater than nominal.

IT General Controls

- Important for compliance with SOx and MAR
- Categorized as “Key” or “Non-Key”
- Key rated as H, M, or L
- Aspects:
  - Impacts on Financial Reporting
  - Threats and Risks
  - Compensating Controls
**IT General Controls**

- Incident Management
- Change Management
- Release Management
- Solutions Delivery Methodology (SDLC)
- Strategic Planning
- Identity and Access Management
- Operations Management
  - Mainframe
  - Distributed
- Physical Security
- Risk Management

---

**Risk Analysis**

- Qualitative: identify the major threats to which an enterprise is exposed. Qualify which risks are worth protecting against.
  - What could happen?
  - How likely?
  - The impact?
- Quantitative: establish monetary value for the assets and processes, probability of the occurrence, ROI for safeguarding the assets
- **All audits start with an RA of the area being reviewed**
Risk Management Activities

- **Risk Profile**
  - Sets the context for performing the risk assessment.
  - Provides guidance on how to perform the assessments by documenting the risk domains, tolerances, objectives and a measurement scale.

- **Risk Assessment**
  - Identifies the risks and relevant mitigating controls.
  - Calculates the residual risks.
  - Determines the risk remediation recommendations.

- **Risk Report**
  - Creates summary reports, aggregate reports, and dashboard views.
  - Creates and escalation and exception process / documentation.

- **Risk Monitor**
  - Tracks risk remediation status, providing escalation paths and documentation stores to track implemented and non-implemented recommendations.

---

Risk Management Process

- Identify information resources
- Assess threats and vulnerabilities
- Impact analysis
- Identify risks, evaluate controls
### Identify Information Resources

- **Typical types of assets**
  - Information and data
  - Hardware
  - Software
  - Services
  - Documents
  - Personnel

- **Critical systems - based on business objectives and information assets**

- **System support infrastructures**
  - Operating Systems
  - Database Management Systems
  - Networks
  - Data Centers

### Assess Threats and Vulnerabilities

<table>
<thead>
<tr>
<th>Assets</th>
<th>Threats</th>
<th>Vulnerabilities</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information/Data</td>
<td>Errors</td>
<td>Lack of user knowledge</td>
<td>Incorrect financial statements</td>
</tr>
<tr>
<td>Hardware</td>
<td>Malicious Attacks</td>
<td>Lack of security functionality</td>
<td>Loss of Confidential Data</td>
</tr>
<tr>
<td>Software</td>
<td>Fraud</td>
<td>Poor passwords</td>
<td>Theft, excessive payments</td>
</tr>
<tr>
<td>Documents</td>
<td>Theft</td>
<td>Transmissions not secured</td>
<td>Eavesdropping, data leakage</td>
</tr>
<tr>
<td>Services</td>
<td>Internal / External</td>
<td>Poor service levels / contracts</td>
<td>???</td>
</tr>
<tr>
<td>Personnel</td>
<td>Equipment failure</td>
<td>Lost productivity</td>
<td>???</td>
</tr>
</tbody>
</table>
What do you do with Risk?

Accept: The risk and the potential $$$ fall-out

Avoid: disengage in the activity or find a different approach to the activity that is creating the risk

Transfer: to another department, company or take out insurance

Mitigate: add controls or change the process

Dealing with Risk

Identify information resources
Assess threats and vulnerabilities
Impact analysis
Identify risks, evaluate controls

Lifecycle of a Control

Assess Risk
Identify Need for Control (or a change to a control)
Continuous Improvement
Design Control
Implement Control
Perform Internal Controls Evaluation
The Universe

Residual Risks

CONTROLS

Inherent Risks

- Client
- People
- Operational Complexity
- Credit
- Technology
- Competition

Legal & Regulatory
Reputational
Significance

Evaluate Controls

- Controls are countermeasures to inherent risk
- Inadequate existing controls require design of new ones

- Inherent control: design strength and likelihood of effectiveness

- Preventive vs. detective
- Manual vs. automated
- Ad hoc

- Residual risk: after applying the inherent control, the remaining risk not covered
The impact/severity of the risk is proportional to the business value of the loss/damage.

A fundamental problem of risk management is to achieve a cost-effective balance between risk and countermeasures.

An additional factor is the level of risk that management will accept (risk appetite).

Cost / Risk

Identify information resources
Assess threats and vulnerabilities
Impact analysis
Identify risks, evaluate controls

Risk Assessment Activities

Determine areas to include within the scope
Leverage results of previous assessments/audits to promote efficiencies
Conduct facilitated sessions with key business and IT process owners to identify and understand IT risks.
Aggregate the results to develop the risk universe
Create risk evaluation criteria to assist in the prioritization of risks
Components of Risk Assessment

Risks and risk impact:
- Identify risk
- Classify the risk
- Prioritize the risk
- Evaluate the risk and impact

Provide Management with:
- Results
- Recommendations

Management review:
- Risk identification
- Risk analysis
- Predetermined organization objectives

Scope of an Assessment

Hardware
- Changes in Operating Environment
- Changes in Technology
- Meet future goals

Projects
- Legislation
- New Products
- Vendors

Software
- Patches
- Upgrades
- Changes
- Future goals

System
- New Development
- Project ROI
- Unauthorized Changes

Information
- Business continuity
- Expanded Operations
- Mergers

People
- Organization structure
- Mgmt competency
- Turnover
- Hackers
- Disgruntled Employees
- Vendors

Other assets
- Policies & procedures
- Telecommunications
- Internet

Data
- Confidentiality
- Accuracy
- Integrity
Data Integrity Risks

Data / systems
- Critical to operations
- Contain confidential information

Data integrity: risk of unauthorized access:
- If the data is changed
  - will it alter the value of corporate assets?
  - will it cause a change in the outcome of a basic business function?
- Disclosure of information represents a risk of damage to the company or an individual

Systems support the critical data
- Legacy systems
- Under reconstruction

IT Risk Assessment Steps

1 Scope Definition
2 Threat Identification
3 Vulnerability Identification
4 Control Analysis
5 Likelihood Determination
6 Impact Analysis
7 Risk Determination
8 Control Recommendations
IT Risk Assessment Steps

1. Scope Definition
   - What:
     - IT Infrastructure
     - Resources
     - IT RA document
     - Business model, P&P, goals & objectives
   - How:
     - Questionnaires
     - Interviews
     - IT Strategic Plans
     - Documentation Reviews

2. Threat Identification
   - What:
     - Object
     - Person
     - Outside entity
     - New technology
     - Business environment
   - How:
     - History of attacks
     - Intelligence reports
     - Articles
     - Cyber chatter

3. Vulnerability Identification
   - What:
     - Flaw or weakness in security
     - Design flaws
     - Control flaws
     - Documentation
   - How:
     - Previous Risk Assessments
     - Audit Comments
     - Security Reviews

4. Control Analysis
   - What:
     - Current Controls
     - Technical
     - Non-Technical
     - Planned Controls
   - How:
     - Audit Comments
     - CobIT 5.0

5. Likelihood Determination
   - What:
     - Threat source motivation
     - Threat capacity
     - Current Controls
   - How:
     - Interviews with IT
     - Interviews with Management
     - Rank as High, Medium, Low

6. Impact Analysis
   - What:
     - Mission
     - Asset Criticality
     - Data Sensitivity
     - Data Criticality
   - How:
     - Interview information owners
     - Analyzing data sensitivity
Joining Two Aspects

<table>
<thead>
<tr>
<th></th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood</td>
<td>&lt;10%</td>
<td>10% - 40%</td>
<td>&gt; 40%</td>
</tr>
<tr>
<td>Impact</td>
<td>&lt; $1 MM</td>
<td>$1 - $5 MM</td>
<td>&gt; $5 MM</td>
</tr>
</tbody>
</table>

Risk Determination

- What
  - Likelihood of threat
  - Extent of Impact
  - Controls Adequacy

- How
  - Risk Matrix
  - Determine Probability
  - Determine Severity

IT Risk Assessment Steps

7 Risk Determination

8 Control Recommendations

- What
  - Policies & Procedures
  - Human Resources
  - Hardware / Software Controls

- How
  - Audit Comments
  - CobiT 5.0
Control Recommendations

- Categorize weaknesses and prioritize the remediation
- Conduct the assessment again
- Control weaknesses not mitigated could have negative impact on the organization
- Progress on the remediation should be monitored and reported
- Remediation strategy must be adopted, approved and reviewed by senior management

The Audit Plan

Goals and Objectives

- Start with the organization’s goals and objectives
- Do not propose irrelevant projects and not providing insight management will truly care about

Interviews

- Start with Senior Manager or Director level employees
- Determine how their roles and responsibilities help the organization achieve its goals and objectives
- Obtain an understanding of how they are spending most of their time

Analyze and Assess

- Group risk information by risk categories or themes
- Summarize the responses and information collected for this risk into a two or three sentence description
### The Audit Plan

#### Determine Likelihood / Impact Analysis

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The CAE should be able to informally assess likelihood and impact</td>
<td>Vet the analysis with management and obtain their feedback and suggestions</td>
</tr>
</tbody>
</table>

#### Benchmark With External Research and Peers

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current and emerging risk topics are reflected in your analysis. Industry trade journals, periodicals, and blogs, and end with major news publications</td>
<td>Talk with other CAEs in your industry</td>
</tr>
</tbody>
</table>

#### Validate with Executive Management

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share all of the work with those that know the company the best and have them validate the information</td>
<td>Executive management team should be the ones that can best articulate the biggest risks of the organization</td>
</tr>
</tbody>
</table>

### Now What?

- Use outside resources to calibrate internal findings
- Map to what the company has done
- Prepare risk analysis for presentation to the Audit Committee
**Outside Resources - CEB**

<table>
<thead>
<tr>
<th>CEB – Internal Audit Strategic Planning Process</th>
<th>XYZ Internal Audit Activity</th>
</tr>
</thead>
</table>
| 1 Conduct an external and internal environmental scan | • Conduct risk discussions with key contacts at XYZ divisions, including subsidiaries  
• Assess recent audit results and exceptions  
• Compare risks with external sources and publications (Big Four accounting firms, CEB, etc.) |
| 2 Understand corporate strategic objectives | Obtain and incorporate from XYZ strategic communications and meeting (examples include):  
• Quarterly Leadership Management Council Forums  
• 20xx/20xx XYZ Strategic Imperatives  
• XYZ Purpose  
• Mission and Vision Statements |
| 3 Assess assurance efforts by other teams | Meet with Enterprise Risk Management (ERM) and Government Programs Compliance to share and compare risk results |
| 4 Formulate and confirm strategic imperatives | Using inputs from steps 1 -3, incorporate XYZ’s strategic objectives in the development of the Master Audit Plan (MAP) |
| 5 Assess skills, organizational structure, and readiness | Review the following:  
• Audit Resources (skills, expertise, experience, etc.)  
• Requirements of MAP  
• Availability of internal and external resources |

---

**Outside Resources - CEB**

<table>
<thead>
<tr>
<th>CEB – Internal Audit Strategic Planning Process</th>
<th>XYZ Internal Audit Activity</th>
</tr>
</thead>
</table>
| 6 Develop and integrate an operating plan | Finalize the MAP incorporating the following:  
• Detailed audit universe schedule  
• Updated templates to support MAP  
• Monthly MAP forecast with Audit Committee due dates |
| 7 Develop the budget | • Each audit team develops a budget of hours to support its section  
• Temporary staff is hired to ensure adequate staffing is maintained |
| 8 Create success metrics and a performance monitoring system | Establish the following:  
• MAP is tracked by scheduled, in-process, and completed work  
• Client satisfaction surveys are sent and tracked on a 5 point scale  
• CPEs are tracked to support staff training and growth  
• Evaluations are completed for each staff. Quality audit reviews are completed throughout the year |
| 9 Communicate Internal Audit strategy broadly | Audit Services strategy is communicated by:  
• Weekly Audit Services senior leadership meetings, manager meetings, and monthly staff meetings  
• Yearly planning meetings and Quarterly Townhalls  
• Review with Executive Vice Presidents and above prior to finalization of MAP  
• Audit Committee meetings five times a year |
| 10 Monitor and adapt Internal Audit strategy | Continuously assess progress through the following:  
• Monthly management meetings  
• Reporting (open exceptions, audit completion percentage)  
• Revisiting Risk Assessment as part of each engagement and making adjustments as needed |
### Outside Resources - Comparison

<table>
<thead>
<tr>
<th>XYZ Internal Audit Risk Assessment 2015</th>
<th>Top Audit Risks from Leading Industry Experts</th>
<th>Corporate Executive Board</th>
<th>PwC</th>
<th>AON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business - Financial and Operational</td>
<td>Changing Customer Needs and Behaviors</td>
<td>Strategic Change Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>Digital Marketing</td>
<td>Strategic Change Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government Programs - Medicaid and Medicare</td>
<td>Changing Customer Needs and Behaviors</td>
<td>Strategic Change Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Special Change</td>
<td>Strategy Change</td>
<td>Increasing Competition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sustainability</td>
<td>Sustainability</td>
<td>Foundation Instability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Increased Regulation Oversight</td>
<td>Cost of Compliance with Multiple Regulations</td>
<td>Risk Instability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>Regulatory Changes and Elevated Stakes</td>
<td>Risk Instability</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### KPMG 2015 Risks

**Top 10 key risks in 2015**

1. Cybersecurity
2. Regulatory compliance
3. Antibribery/Anticorruption
4. International operations
5. Third-party relationships
6. Mergers, acquisitions, and divestitures
7. Strategic alignment
8. Integrated and continuous risk assessment
9. Data analytics and continuous auditing
10. Talent recruitment and retention
Audit Response

<table>
<thead>
<tr>
<th>Key Risk Areas</th>
<th>Audit Observations</th>
<th>2015 Audit Plan Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Business – Retail and group</td>
<td>Throughout 2014, management enhanced its operations to address these challenges and plan for 2015 open enrollment, which will include the re-enrollment of XYZ 2014 Exchange membership.</td>
<td>In 2015, Audit Services will continue to monitor and review the remediation of these control gaps. In addition, Audit Services will be performing audit work on XXXXX.</td>
</tr>
<tr>
<td>Government Programs</td>
<td>XYZ and its subsidiaries continue to work through the many challenges faced when implementing new products, including working with new vendors and ensuring continued compliance with regulations.</td>
<td>Audit Services will continue to partner with Government Programs Compliance and the Government Programs Division to audit processes for Medicare and Medicaid.</td>
</tr>
<tr>
<td>Supplier Oversight</td>
<td>Management continues to look for viable options for transferring processing functions to strategic business partners. Reliance on third parties for key business activities increases risks related to the extended enterprise.</td>
<td>Continue to perform reviews of key outsourced business functions with a particular focus on suppliers that handle and store sensitive XYZ data. Through the use of detailed questionnaires and onsite visits (if necessary), this effort provides coverage on eight IT security domains including workstation security, user access administration, and disaster recovery controls.</td>
</tr>
<tr>
<td>Design and Execution of IT Controls</td>
<td>IT is challenged with delivering solutions and services in a fast-paced and changing regulatory environment. There are greater demands from external customers and regulatory agencies to demonstrate effective IT controls and governance. With regards to external threats, cyber security risks and the potential disruption of core operations remain top concerns.</td>
<td>In 2015, Audit Services will assess whether the general IT controls foundation achieved over the last several years continues to be maintained. Oversight of remediation activity over External Data Exchanges and Government programs interface controls will be conducted. Audit Services will continue to monitor federal and industry guidance on cyber security. This effort will support the HIPAA Security, SOC 1, and SOC 2 engagements. Additionally, audit work will be performed to address patch management, firewalls, and mobile device controls.</td>
</tr>
</tbody>
</table>

Audit Plan

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Description</th>
<th>Audit</th>
<th>Hours</th>
<th>Start</th>
<th>End</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design and Execution of IT Controls</td>
<td>The general IT controls foundation achieved over the last several years continues to be maintained. Oversight of remediation activity over External Data Exchanges and Government programs interface controls will be conducted. Audit Services will continue to monitor federal and industry guidance on cyber security. This effort will support the HIPAA Security, SOC 1, and SOC 2 engagements. Additionally, audit work will be performed to address patch management, firewalls, and mobile device controls.</td>
<td>ITG General Controls</td>
<td>400</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Security Review</td>
<td>250</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identity and Access Management</td>
<td>1300</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile Device Security Review</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Patch Management Review</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supplier Assessments</td>
<td>500</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOC 1 Coordination</td>
<td>150</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOC 2 Coordination</td>
<td>150</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Exchange Review</td>
<td>350</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Checking the Quality of the MAP

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Has internal audit spent time in the business to develop an understanding of key issues?</td>
</tr>
<tr>
<td>2</td>
<td>Does the scope of work in the annual MAP plan meet the requirements of the Audit Charter?</td>
</tr>
<tr>
<td>3</td>
<td>Does the annual audit plan align with the organization's strategies and key risks?</td>
</tr>
<tr>
<td>4</td>
<td>Has internal audit undertaken a risk assessment as part of the planning process?</td>
</tr>
<tr>
<td>5</td>
<td>Does the annual audit plan consider changes to the organization’s operating environment?</td>
</tr>
<tr>
<td>6</td>
<td>Does the annual audit plan consider the work of other assurance providers?</td>
</tr>
<tr>
<td>7</td>
<td>Is the annual audit plan dynamic and flexible?</td>
</tr>
<tr>
<td>8</td>
<td>Have senior management provided input to the annual audit plan?</td>
</tr>
<tr>
<td>9</td>
<td>Has senior management and the audit committee agreed to the annual audit plan?</td>
</tr>
<tr>
<td>10</td>
<td>Does internal audit have the resources to deliver the annual audit plan?</td>
</tr>
</tbody>
</table>