Keeping the IT Audit Function Relevant
WHAT WE WILL COVER TODAY

- The Critical Asset Perspective
- The IT Audit Function
- Strengthening the IT Auditor’s Position
The Critical Asset Perspective
IT AUDIT FOCUS

• Scope and compliance requirements dictate technology needs
• Processes evaluated against policies and functional focus
• Integration and communication are afterthoughts
IT AUDIT FOCUS

ISACA Information Technology Assurance Framework (ITAF)

- Focus is on process of performing the audit than on the technical/business aspects of the IT audit
- Several standards address certain types of organizations or certain aspects of IT (HIPAA, GLBA, NIST, etc.)


- **IT AUDIT FUNCTION FOCUS CENTERED ON SCOPE AND COMPLIANCE**
ENTERPRISE SUPPORT FOCUS

- Technology portfolio as a whole becomes main subject of audit
- Enterprise strategy reviewed as cornerstone for process development
- Audit of process reviews portfolio functionality, integration, communication, and commitment
Audit reveals paradigm shift (compliance to commitment based)
Standards provide practical context of business use, support, and goals
All actions audited are aligned with and dependent on enterprise strategy
BEW Global works in cooperation with customers to plan, implement and maintain a **Critical Asset Protection Program (CAPP)** that clearly defines what assets are deemed most important to the customer organization based on revenue, income, reputation and core operational impact.
The IT Audit Function
IDENTIFYING AND MITIGATING RISK

• CRITICAL ASSET RISKS
  – What are our critical assets?
  – What is the value of our critical assets?
  – What is the probability of these critical assets being compromised?
  – What risks exist in having these critical assets?
  – What level of risk can we safely/ultimately accept?

• CRITICAL ASSET CONTROLS
  – What controls do we have in our IT inventory/portfolio?
  – Do these controls protect our critical assets?
  – Do these controls address our risks (based on levels/priorities)?
  – What impact do these controls have on business operations?
  – What level of disruption to business processes can we safely/ultimately accept?
IDENTIFYING AND MITIGATING RISK

**BUSINESS SUPPORT NEEDS**

- CAPP SCOPE DESIGN
- CRITICAL ASSET PRIORITY LIST
- GAP ANALYSIS
- IT AUDIT
- ASSET INVENTORY
- RISK ASSESSMENT
- RISK TREATMENT PLAN
- CAPP SCOPE UPDATE

**BEW GLOBAL CAPABILITIES**

- Product Health Check
- DLP Program Health Check
- DLP Program Design
- Security Strategy Program Design
- Security Strategy Program Evaluation
- Vulnerability Scanning
- Security Assessments
- Security Technology Asset Inventory Review (STAIR)
- Critical Asset Valuation Risk Model (CAVRM)
- ISO 27001 Gap Analysis
- ISO 27005 Risk Assessment
- ISO 27001 Certification Assistance
RISK ASSESSMENT AS THE FOUNDATION FOR ANY AUDIT

BEW GLOBAL’S ISO 27001-27005 RISK ASSESSMENT METHODOLOGY

Phase 1
- Determine scope of Information Security Management System (ISMS)
- Identify key assets, processes, and classification criteria to develop the following deliverables: policy, scope, asset inventory, risk treatment plan
- Develop risk acceptance criteria and associated scale
- Create threat & vulnerability register

Phase 2
- Identify risk, and then value risks based on confidentiality, integrity, and availability
- Analyze risks by applying likelihood & probability impact estimates
- Develop a Risk Treatment Plan (RTP)
- Summarize preliminary results at completion of onsite work

Phase 3
- Generate initial report with analysis of findings for client review
- Complete final report & recommendations

BEWGLOBAL.COM
Strengthening the IT Auditor’s Position
<table>
<thead>
<tr>
<th>ACTION</th>
<th>RELEVANT AREA</th>
<th>NOT RELEVANT AREA</th>
</tr>
</thead>
<tbody>
<tr>
<td>MANAGE</td>
<td>PEOPLE</td>
<td>TECHNOLOGY</td>
</tr>
<tr>
<td>AUDIT</td>
<td>PROCESS</td>
<td>PRACTICE</td>
</tr>
<tr>
<td>THINK</td>
<td>CRITICAL ASSETS</td>
<td>PLATFORMS</td>
</tr>
<tr>
<td>SUPPORT</td>
<td>BUSINESS UNITS</td>
<td>SOLUTION OWNERS</td>
</tr>
<tr>
<td>STRENGTHEN</td>
<td>BUSINESS OPERATIONS</td>
<td>TECHNOLOGY FOOTPRINT</td>
</tr>
<tr>
<td>ACHIEVE</td>
<td>BUSINESS GOALS</td>
<td>COMPLIANCE</td>
</tr>
</tbody>
</table>
ISO 27000 & PDCA

INTERNAL FACTORS
PEOPLE
PROCESS
CRITICAL ASSETS
BUSINESS UNITS
BUSINESS OPERATIONS
BUSINESS GOALS

CONSIDERATIONS
TECHNOLOGY
PRACTICES (BEST)
PLATFORMS
SOLUTION OWNERS
TECHNOLOGY FOOTPRINT
COMPLIANCE
VALUE ADD

- Identifies organizational strengths AND weaknesses
- Ensures compliance (general & specialized standards)
- Mitigates risk
- Protects critical assets
- Reduces inefficiencies
- Demonstrates true ROI
- Enables the business decision maker’s position
QUESTIONS?