Even though IT risks are on the Board’s agenda more than ever before, few Boards understand the full degree of their operational dependence on computer systems and the role that IT plays in shaping their firm’s strategies. It is therefore increasingly critical that Internal Audit (IA) focus their IT audit effort on the things that matter and communicate those issues in a way that the Board can understand them.

Our IT IA services can better enable your organisation and internal audit function, if applicable, to navigate IT challenges, manage organisation-wide risks, and elevate the role of IA. Our IT IA services allow the stakeholders of your organisation to meet their responsibilities and accordingly address their concerns of the IT in your organisation.

**CIO**
**Responsibility:**
- Partnering with the Business to drive growth and efficiency
**Concerns:**
- Manage the spiraling cost of technology
- Delivering state of the art systems

**Compliance/General Counsel**
**Responsibility:**
- Provides guidance
- Interpret the existing and pending regulatory rules to senior management
**Concerns:**
- Impact of new domestic or international rules (e.g., Privacy, Data Protection Laws)

**CFO**
**Responsibility:**
- Creating a sound framework of financial operational controls
**Concerns:**
- Accountability
- Segregation of Duties
- Compliance
- Regulatory Reporting

**CTO/CISO**
**Responsibility:**
- Building flexible secure systems and infrastructure
- Providing 24/7 access to systems and data
**Concerns:**
- Managing the risks of social networking, personal devices, identify theft, interoperability, mobility, availability, third party management, mobile banking and data leakage or PI loss.

**Audit Committee**
**Responsibility:**
- Proper resources
- Training
- Evaluate control structure
- Oversees risks

**CEO**
**Responsibility:**
- Sets the strategic direction of the Firm
- Develops overall governance and control framework
**Concerns:**
- Reputational, regulatory, financial, operational and technology risk

**PwC can help you:**
IT IA services help our clients extend their internal audit oversight and performance addressing IT risks as well as broader organization—wide business risks. We help connect IT and IA to gain a greater understanding of the risks and opportunities that come with today’s systems, applications and other technologies. Our talented practitioners possess the necessary business and technical skills that enable us to deliver assessments in the areas of IT Governance¹, IT Applications² and IT Technical Controls³.

**Typical IT risks and potential impacts**

**Impact of failure**
- IT risks are not identified, escalated and clearly communicated at Board level; history of failed projects.
- IT strategy not aligned with the business strategy.
- Regulatory sanction and reputation damage.
- Higher cost of compliance.
- Poor controls in key business systems can lead to poor quality management information, fraud and difficulties complying with regulation.
- Failed or delayed projects leading to increased cost.
- Benefits are not leveraged across the organisation.
- Critical business systems unavailable, financial loss through internal or external fraud, reputation damage, identity theft or regulatory sanction.
- Successful hacking attempts.

**If you:**
- Do not have an IT audit plan based on a framework that results in a complete, top down and risk-based scope of work.
- Are not confident that your Internal Audit department is able to identify IT risks and communicate findings in a way that these are understood and taken seriously by the Board.
- Do not have the skills and experience to deliver IT audit work across the business.
**PwC IT IA Methodology**

**Technology Assurance Wheel:**

As part of our IA methodology, the technology assurance wheel identifies significant IT risks. The impact of these risks is both operational and financial in nature and as such represents a key area of focus for both IT and financial management within any organisation. Well run organisations manage these risks on an ongoing basis.

**IT Risk & Diagnostic/Benchmark (ITRD) tool**

The reliance on IT systems by organisations is on an increasing trend and as a result organisations are becoming increasingly aware of the inherent risks from such reliance. Understanding your technology risks and how they impact your business objectives is paramount. The pace of IT change, regulatory pressures and increasing dependency on IT also represent a significant challenge for companies in an effort to remain competitive and comply with existing regulations.

Our IT IA services include a peer group comparison that will provide you with an insight into how other industries are managing their IT and help you to identify areas for improvement. We compare your organisation's IT risk profile against peers in key areas, quickly producing a benchmark of relative risk maturity against up to 600 other organisations.

**IT strategy and governance**

1. **Strategic decision-making**
   1.2 IT Strategy
   1.3 Decision making
   1.4 Emerging technology
   1.5 ERP strategy
   1.6 Centralisation and standardisation

2. **IT governance**
   2.1 Governance structure
   2.2 IT policies and standards
   2.3 Cost and charge back
   2.4 IT risk management
   2.5 IT compliance
   2.6 IT performance management

3. **IT management**
   3.1 IT management information
   3.2 Project portfolio/programme management
   3.3 People management
   3.4 Third party management
   3.5 Software licensing
   3.6 Hardware asset management

**IT processes and procedures**

4. **Systems quality**
   4.1 Systems quality and business intelligence
   4.2 Data quality
   4.3 End-user computing
   4.4 Project management and benefits realisation
   4.5 Acquiring and developing new technology

5. **Systems support and change**
   5.1 Systems support capability
   5.2 Change management process
   5.3 Promotion (and access) to live

6. **IT operations**
   6.1 Physical data centre security
   6.2 Service delivery and problem management
   6.3 Disaster recovery and continuity
   6.4 Data retention

7. **Information security**
   7.1 Security management
   7.2 Security awareness and training
   7.3 Identity and access management
   7.4 Monitoring unusual and privileged access
   7.5 Threat and vulnerability management
   7.6 Data loss prevention
## Additional IT services

<table>
<thead>
<tr>
<th>IT Governance</th>
<th>IT Applications</th>
<th>IT Technical Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provide an assessment of critical firm-wide processes, such as:</strong></td>
<td><strong>Provide application assessments from the following perspectives:</strong></td>
<td><strong>Perform comprehensive IT control assessments of critical infrastructure or processes, such as:</strong></td>
</tr>
<tr>
<td>• IT Governance</td>
<td>• Pre-Implementation Reviews</td>
<td>• Attack and Penetration Testing</td>
</tr>
<tr>
<td>• IT Risk and Security Assessments</td>
<td>• Data Assurance: Conversions or Large Scale System Migrations</td>
<td>• Network Security (e.g., firewalls, routers)</td>
</tr>
<tr>
<td>• Business Continuity and Disaster Recovery Planning Assessments</td>
<td>• Application Control Reviews</td>
<td>• Web Application Security</td>
</tr>
<tr>
<td>• Regulatory Compliance and implementation with various security frameworks (e.g., ITIL, COBIT, ISO27001)</td>
<td>• Analysis and User Provisioning Evaluations</td>
<td>• Wireless and Remote Access Security</td>
</tr>
<tr>
<td>• Data Privacy Assessments (e.g. PCI)</td>
<td>• SDLC and Project Management</td>
<td>• Mobile Computing</td>
</tr>
<tr>
<td>• Third-Party Vendor Assessments</td>
<td>• ERP Systems Assessments (e.g., Navision, SAP and Oracle)</td>
<td>• Platform and Operating System Security (e.g., Unix, AIX, LINUX, Windows, IBM Mainframe, IBM iSeries)</td>
</tr>
<tr>
<td>• Designing or assessing an IT risk metrics program</td>
<td>• Computer Assisted Audit Techniques and Continuous Monitoring Processes</td>
<td>• Database Security (e.g., Sybase, Oracle, SQL, DB2)</td>
</tr>
<tr>
<td>• Outsourcing/Off-shoring Strategy</td>
<td>• End User Computing</td>
<td>• Program and System Change Control</td>
</tr>
<tr>
<td>• Procurement and Sourcing</td>
<td>• Identity and Access Management</td>
<td>• Computer Operations (e.g., Data &amp; software backup, problem management, system monitoring, job scheduling)</td>
</tr>
<tr>
<td>• Security Crises Management</td>
<td></td>
<td>• Data Center Physical Security and Environmental Controls</td>
</tr>
</tbody>
</table>

---

**For more information please contact:**

- **George Lambrou**
  Partner
  Risk Assurance Consulting
  T: +00357 22 555 728
  george.lambrou@cy.pwc.com

- **Tassos Procopiou**
  Partner
  Consulting
  T: +357 - 22 555 750
  tassos.procopiou@cy.pwc.com

- **Demos Demou**
  Manager
  Risk Assurance Consulting
  T: +00357 22 555 056
  demos.demou@cy.pwc.com

- **Efthyvoulos Efthyvoulou**
  Manager
  Risk Assurance Consulting
  T: +00357 22 555 460
  efthyvoulos.efthyvoulou@cy.pwc.com

---

**PwC Cyprus**

Julia House, 3 Themistocles Dervis Street, CY-1066 Nicosia, Cyprus
P O Box 21612, CY-1591 Nicosia, Cyprus
T: +357 - 22555000, F: +357 - 22555001
www.pwc.com.cy/technology-consulting

---

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2015 PricewaterhouseCoopers Ltd. All rights reserved. PwC refers to the Cyprus member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.