Managing technology risk is now a business priority
Global Regulatory Technology Risk Requirements
Regulatory technology risk requirements landscape have changed over the past 3 years

- U.S. Securities and Exchange Commission (SEC)
- Federal Deposit Insurance Corporation (FDIC)
- Consumer Financial Protection Bureau (CFPB)
- Financial Conduct Authority (FCA)
- Prudential Regulation Authority (PRA)
- Financial Services Agency (FSA), Japan
- China Securities Regulatory Commission (CSRC)
- China Insurance Regulatory Commission (CIRC)
- China Banking Regulatory Commission (CBRC)
- Monetary Authority of Singapore (MAS), Singapore
- Reserve Bank of India (RBI)
- Insurance Regulatory and Development Authority (IRDA)
- Australian Prudential Regulation Authority (APRA)
- Federal Financial Supervisory Authority (BaFin), Germany
- Autorité des marchés financiers (France) (AMF), France
- Swiss Financial Market Supervisory Authority, Switzerland
The interplay of new technology risk regulation with other market changes is driving wide-ranging business impacts.

**Impact of regulation: Overview**

- **Change-driven business impacts**
  - **Strategic Impacts**
    - Attractiveness of markets, business models and portfolios under new rules
  - **Operational effectiveness and cost management**
    - Driven by strategic business choices and new reporting/transparency requirements
  - **Organisation, governance and culture**
    - Incentives and governance rules the subject of more intense regulatory interest

- **External Environment**
  - Slow growth
  - Depressed yields

- **FS Regulations**
  - Technology Risk
  - FATCA

- **Risk Mgmt**
  - AML
  - Capital & liquidity

- **Exec Compensation**
  - Disclosure
  - Payment structures

- **Tax**
  - Structuring/levies
  - Reserving

- **Accounting policies**
  - GAAP changes

- **PwC**
MAS Technology Risk Management Notices and Guidelines
The new MAS Technology Risk Management Guidelines (TRMG) have been enhanced to help financial institutions’ improve oversight of technology risk management and security practices.

**Technology Risk Management Notice and Guidelines**

- The Notice and Guidelines were issued on 21 June 2013.
- Notice will be effective on 1 July 2014.
- All 12 notices tied to the Singapore Act and Laws will impact:
  - All Financial Institutions (FIs) (See Appendix for definitions)
  - Includes all IT systems

Non compliance to the Notice can result in:
- Financial penalties
- Reputational damage
- Revocation of licence to operate in Singapore
What are the implications of the Notice?

1. Perform a Business Impact Analysis to identify Critical Systems
2. Test your Disaster Recovery (DR) Plans are robust
3. Encrypt customer data to protect
4. Active: Active infrastructure
5. Real time monitoring and reporting procedures

A FI shall put in place a framework and process to identify critical systems

Recovery Time Objective (RTO) of ≤ 4 hours for critical systems

A FI shall implement IT controls to protect customer information from unauthorised access or disclosure

High availability for critical systems ≤ 4 hours of unscheduled downtime

Inform MAS of major security incidents, systems malfunction within 60 minutes and submit root cause with 14 days
With the new TRM Notice and Guidelines, six grouped areas that impact your business were identified.

1. Notice
2. System Availability, Incident and Capacity Management
3. Operational Infrastructure Security and Access Management
4. Development and Change Management
5. Mobile Online Services
6. Others
**Notice**

<table>
<thead>
<tr>
<th>Consultation Paper</th>
<th>TRMG 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single Notice</strong></td>
<td>Each type of FI (banks, insurance company, brokers, etc.) is issued one Notice, but the contents is the same.</td>
</tr>
<tr>
<td><strong>Redefinition of following terms:</strong></td>
<td></td>
</tr>
<tr>
<td>- Critical system: Failure of which will cause significant disruption into the operations of the FI or materially impact the FI’s service to its customers</td>
<td></td>
</tr>
<tr>
<td>- System malfunction: failure of any of the FI's critical systems</td>
<td></td>
</tr>
<tr>
<td>- Relevant incident: System malfunction or IT security incident, which has a severe and widespread impact on the FI's operations or materially impacts the FI's service to its customers</td>
<td></td>
</tr>
<tr>
<td><strong>Notification to MAS within 30 minutes for all IT Security Incidents</strong></td>
<td>Notification: no later than 1 hour upon discovery of a relevant incident. Upon discovery refers to after the FIs have ascertained the nature and magnitude of an IT incident meets the criteria set out in the Notice.</td>
</tr>
<tr>
<td><strong>Submission of root cause analysis within one month</strong></td>
<td>Root cause analysis changed to: submit within 14 days of discovery. Can request for extension.</td>
</tr>
</tbody>
</table>

“The Notice has clear definitions and are legally binding requirement for FI’s”
### System Availability, Incident and Capacity Management

<table>
<thead>
<tr>
<th>Consultation Paper</th>
<th>TRMG 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieve near zero system downtime for critical systems</td>
<td>Achieve high availability for critical systems.</td>
</tr>
<tr>
<td>Public announcement of major incidents should be made in a timely manner</td>
<td>This requirement was removed. Expectation BCP will address this matter.</td>
</tr>
<tr>
<td>Conduct quarterly trend analysis</td>
<td>Removal of quarterly trend analysis.</td>
</tr>
<tr>
<td>No Requirements</td>
<td>FI should inform MAS as soon as possible in the event that a critical system has failed over to its disaster recovery system.</td>
</tr>
</tbody>
</table>
# System Availability, Incident and Capacity Management

<table>
<thead>
<tr>
<th>Consultation Paper</th>
<th>TRMG 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>No requirement to encrypt USB disks.</td>
<td>Encrypt USB disks containing sensitive or confidential information before transporting to off-site for storage. The encrypting of sensitive information should be performed on all mediums that are transported off-site.</td>
</tr>
<tr>
<td>No requirement for timeframe of review.</td>
<td>Evaluate the recovery plan and incident response procedures at least annually.</td>
</tr>
<tr>
<td>No detailed requirements</td>
<td>New requirements:</td>
</tr>
<tr>
<td></td>
<td>• FI to ensure that indicators such as performance, capacity and utilisation are monitored and reviewed.</td>
</tr>
<tr>
<td></td>
<td>• FI should establish monitoring processes and implement appropriate thresholds to provide sufficient time for the FI to plan and determine additional resources to meet operational and business requirements effectively.</td>
</tr>
</tbody>
</table>
**Operational Infrastructure Security and Access Management**

<table>
<thead>
<tr>
<th>Consultation Paper</th>
<th>TRMG 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement 2FA for privileged users</td>
<td>Implement strong authentication mechanisms for privileged users.</td>
</tr>
<tr>
<td>Quarterly Vulnerability Assessment requirement</td>
<td>Frequency of vulnerability assessment is removed. Expectation to perform annual penetration test is still required.</td>
</tr>
</tbody>
</table>

“Strong authentication on customer and transactional processing”
"Non-production environments can connect to the internet"

<table>
<thead>
<tr>
<th>Consultation Paper</th>
<th>TRMG 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only allowed production environment to be connected to the Internet</td>
<td>Non-production environment is now allowed to connect to the internet provided a risk assessment has been performed and appropriate controls are in place.</td>
</tr>
</tbody>
</table>
“Magnetic stripes are allowed”

<table>
<thead>
<tr>
<th>Consultation Paper</th>
<th>TRMG 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction-signing for high-risks / high-value transactions</td>
<td>Online financial systems servicing institutional investors, can use alternate controls, if assessed to be equivalent or better than using token-based mechanisms to authorise transaction.</td>
</tr>
<tr>
<td>Magnetic stripes were not allowed</td>
<td>If, for interoperability reasons, transactions could only be effected by using information from the magnetic stripe on a card, the FI should ensure that adequate controls are implemented to manage these transactions.</td>
</tr>
</tbody>
</table>
## Others

<table>
<thead>
<tr>
<th>Consultation Paper</th>
<th>TRMG 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archival of cryptographic key</td>
<td>The requirement that cryptographic keys should only be used for a single purpose, and archival of keys has been removed. Expectation a Key Management policy should cover lifecycle of keys.</td>
</tr>
<tr>
<td>Reliability and resiliency</td>
<td>Requirement to implement mirrored / parity redundancy for RAID (Redundant Array of Independent Disk), as well as allocation and configuration for hot spares removed.</td>
</tr>
<tr>
<td>Requirement for IT Audit to validate and verify issues raised by MAS inspection</td>
<td>Removal of IT audit (IA) requirement. Expectation that IT Audit will review MAS findings. It is good practice for IA to be aware of relevant issues and consider as part of their risk universe.</td>
</tr>
</tbody>
</table>

**“More areas to focus on”**
### Others

<table>
<thead>
<tr>
<th>Requirement for clearing browser cache after online session did not exist</th>
<th>Added one pre-caution that FI should advise the customer to adopt &quot;clear browser cache after the online session&quot;. Expectation this be part of customer awareness.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Onsite visit to Data centres, or service providers should be performed</td>
<td>Removed, good practice would verify data centres and services providers are compliant to IT Outsourcing requirements and MAS TRM guidelines.</td>
</tr>
<tr>
<td>Verify the authenticity and integrity of the mobile apps</td>
<td>Removed; but transaction-signing should be implemented for authorising transactions.</td>
</tr>
<tr>
<td>PIN should be changed regularly</td>
<td>Added “or when there is any suspicion that it has been compromised or impaired.</td>
</tr>
</tbody>
</table>

**“More areas to focus on”**
Summary of Gap Analysis between IBTRM (Internet Banking and Technology Risk Management) and the new TRM Notice and Guidelines

- 64% New and Enhanced Requirements
- 19% No Change in Requirements
- 17% Clarifications and Statements Update

Applicable to all financial institutions and include all IT systems (inclusive internet).
## System Availability and Incident Management – Impact and Costs

<table>
<thead>
<tr>
<th>Action Required</th>
<th>Framework</th>
<th>Processes</th>
<th>Systems</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define critical systems</td>
<td>✅</td>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Critical Systems need to have high availability with ≤ 4 hours of unscheduled downtime</td>
<td>✅</td>
<td></td>
<td>✅</td>
<td>H</td>
</tr>
<tr>
<td>Mechanism to monitor downtime</td>
<td></td>
<td>✅</td>
<td></td>
<td>May be</td>
</tr>
<tr>
<td>Develop and implement Recovery Plan for Critical Systems (RTO) of ≤ 4 hours. Test &amp; validate annually</td>
<td>✅</td>
<td></td>
<td>✅</td>
<td>H</td>
</tr>
<tr>
<td>Develop and implement incident handling process to achieve 1 hr response upon discovery of “relevant incident”</td>
<td>✅</td>
<td></td>
<td>✅</td>
<td>H</td>
</tr>
<tr>
<td>Develop and capacity management process</td>
<td></td>
<td></td>
<td></td>
<td>May be</td>
</tr>
</tbody>
</table>

Dependency and complexity in involving 3rd party service providers

Legend: L – Low; M – Medium; H - High
Technology Risk Management Guideline vs. IBTRM v3- Themes

1. Technology Risk Management Framework, Roles of Senior Mgmt & Board

2. Enhanced Data Centre Requirements

3. Mobile Online Services

4. Operational Infrastructure Security Management

5. System Availability and Infrastructure Management

6. Others
## Technology Risk Management Framework and Role of Senior Management and the Board

### Key Requirements

- Senior management involvement in the IT decision-making process
- Implementation of a robust risk management framework
- Effective risk register be maintained and risks to be assessed and treated
- Implementation of a employee screening process and annual security awareness training

### What you need to consider

- How is senior management involved in IT decision making and risk management?
- Is there an effective governance in place to ensure the board can make informed decisions?
- Is there a formalised IT risk management framework in place?
- Do employee screening processes include the third parties?
### Enhanced Data Centre Requirements

<table>
<thead>
<tr>
<th>Key Requirements</th>
<th>What you need to consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data centre security should include physical: security guards, card access systems, mantraps and bollards etc.</td>
<td>• Define your data centres and classify the critical systems in scope</td>
</tr>
<tr>
<td></td>
<td>• The TVRA needs cover all possible scenarios</td>
</tr>
</tbody>
</table>

“A robust Threat and Vulnerability Risk Assessment (TVRA) should be performed on critical systems and data centres”
# Mobile Online Services

## Key Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>What you need to consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>A security strategy that included the MAS requirements</td>
<td>Does your current security strategy encompass mobile banking applications?</td>
</tr>
<tr>
<td>Identification of fraud scenarios and payment card fraud counter measures on mobile devices</td>
<td>Does current risk assessment consider mobile banking fraud, mobile-application?</td>
</tr>
<tr>
<td>Sensitive data should be encrypted</td>
<td>What is sensitive data? Is information other than authentication-specific information encrypted on the local device?</td>
</tr>
<tr>
<td>Customers should be educated on security</td>
<td></td>
</tr>
</tbody>
</table>
## Key Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory of software and hardware components and end of support/life (EOS/L)</td>
<td>An asset management database that includes critical systems that can be monitored</td>
</tr>
<tr>
<td>Baseline standards for security configurations</td>
<td>File and system integrity monitoring</td>
</tr>
<tr>
<td>A robust patch management process</td>
<td>How does your current patch management process classify patches? Do you have a patch management strategy that works?</td>
</tr>
<tr>
<td>Real-time monitoring of security events</td>
<td>How are you monitoring your database configuration changes and privileged access?</td>
</tr>
<tr>
<td>Detection of unauthorised changes to critical systems</td>
<td></td>
</tr>
<tr>
<td>Key Requirements</td>
<td>What you need to consider</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Redundancies for single points of failures (Cross-border)</td>
<td>• Are you looking at an Active/Active, or Active/Passive service to meet these guidelines and the Notice. (n+1)</td>
</tr>
<tr>
<td>• Recovery time objective (RTO) and recovery point objective (RPO)</td>
<td>• Have all critical systems and network components (on and offshore) been included?</td>
</tr>
<tr>
<td>• Recovery plan and testing</td>
<td>• Do you have a dedicated CERT and a defined plan for security and major incidents?</td>
</tr>
<tr>
<td>• Incident response procedures</td>
<td>• How and who will manage the public announcements and disclosure?</td>
</tr>
<tr>
<td>• Problem management process (root-cause analysis)</td>
<td></td>
</tr>
</tbody>
</table>
### Others - ITSM (Information Technology Service Management) & Acquisition and Development of Information Systems

<table>
<thead>
<tr>
<th>Key Requirements</th>
<th>What you need to consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A robust IT service management framework should be implemented</td>
<td>• Is there a problem management process in place? Are you using Information Technology Infrastructure Library (ITIL)?</td>
</tr>
<tr>
<td>• Problem management trend analysis</td>
<td>• How and are you reviewing projects and procurements of systems against the needs of the business post implementation?</td>
</tr>
<tr>
<td>• A project management framework should be used and established</td>
<td>• Is a cost benefit analysis and business case developed for all system changes?</td>
</tr>
<tr>
<td>• End user applications should be developed inline with best practices</td>
<td>• Do you know what end user tools/spreadsheets/macros are critical to your business? What was the methodology used to develop these tools?</td>
</tr>
</tbody>
</table>
### Others – Payment Card Security

<table>
<thead>
<tr>
<th>Key Requirements</th>
<th>What you need to consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sensitive payment card data should be encrypted</td>
<td>• Where is your payment card data stored? and is the data encrypted when stored and during processing?</td>
</tr>
<tr>
<td>• Secure chips should be deployed to store sensitive payment card</td>
<td>• Is a FDS in place that uses behavioural scoring?</td>
</tr>
<tr>
<td>• FIs should only allow online transaction authorisation</td>
<td></td>
</tr>
<tr>
<td>• Implementation of Fraud Detection Systems (FDS) with behavioural scoring</td>
<td></td>
</tr>
</tbody>
</table>
Competitive intelligence

Our observation of industry practices
# What you should consider

<table>
<thead>
<tr>
<th>Ensure a robust Technology Risk Management framework is in operation to meet your compliance responsibilities</th>
<th><strong>Scope</strong></th>
<th>Define your scope and risk assess your critical systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Feasibility</strong></td>
<td>Perform a GAP analysis against the TRM Notice and Guidelines</td>
<td></td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>Obtain buy in from key stakeholders</td>
<td></td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>Create a robust governance structure that can guide the development of organisation controls</td>
<td></td>
</tr>
</tbody>
</table>
Banking benchmarking of issues

Reported Issues by Domain

1. Operational Infrastructure Security Management, representing 27% of issues reported.
2. Operational Infrastructure Security Management, representing 27% of issues reported.

The single most popular issue:
Management of IT Outsourcing Risks, representing 7% of issues reported.

Highest number of issues:
Operational Infrastructure Security Management, representing 27% of issues reported.

- Operational Infrastructure Security Management
- Access Control
- Online Financial Services
- IT Service Management
- Oversight of Technology Risks by Board and Senior Management
- Data Centres Protection and Controls
- Systems Reliability, Availability, and Recoverability
- Management of IT Outsourcing Risks
- Acquisition and Development of Information Systems
- Technology Risk Management Framework
- IT Audit
**Insurance benchmarking of issues**

### Reported Issues by Domain

1. Operational Infrastructure Security Management - 31%
2. Acquisition and Development of Information Systems - 13%
3. Online Financial Services - 11%
4. IT Service Management - 10%
5. Oversight of Tech Risks by Board and Senior Mgmt - 10%
6. Access Control - 9%
7. Management of IT Outsourcing Risks - 6%
8. Data Centres Protection and Controls - 4%
9. Systems Reliability, Availability, and Recoverability - 4%
10. IT Audit - 6%
11. Technology Risk Management Framework - 4%

**The single most popular issue:**
Management of IT Outsourcing Risks, representing 6% of issues reported

**Highest number of issues:**
Operational Infrastructure Security Management, representing 31% of issues reported
PwC’s 4-Step MAS TRM Compliance program

<table>
<thead>
<tr>
<th>Assess</th>
<th>Define</th>
<th>Implementation &amp; Rollout</th>
<th>Review &amp; Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review existing framework, processes &amp; systems</td>
<td>Design TRM framework, policies, processes and related controls</td>
<td>Implement Processes &amp; Systems</td>
<td>On-going monitoring of risks and effectiveness of controls</td>
</tr>
<tr>
<td>Gap analysis followed by risk prioritisation</td>
<td>Design governance structure to address new requirements</td>
<td>Set up governance structure and process</td>
<td>Regular Post-implementation review</td>
</tr>
<tr>
<td>Define and design technology solutions</td>
<td>Test effectiveness of solutions and controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Deliverables:
- Gap Analysis results
- Prioritise the issues
- Remediation Action plan
- TRM framework, policies, processes & controls
- TRM governance structure
- Technology Solution Specification
- Rolled out processes solutions
- Training materials and procedure documents
- Pre-implementation test results
- Technology risk reporting and regular test results, e.g. RTO
- Compliance review report
Appendix: Case Studies
Case Studies – Onshore banking

The MAS completed its inspection of Technology and issued a report containing a number of findings.

1. Risk Management of process around critical systems
2. Adhering to 4 hours RTO

PwC were engaged to facilitate the remediation effort:
- understanding the current production environment/architecture for all critical applications and the business lines supported by those applications
- engaging stakeholders from business, IT, technology risk and operational risks in risk assessment workshops
- identify critical information and technology assets residing in each application and analyse possible consequences that bank may face
- review the design effectiveness of internal controls in place
- assess residual risks and facilitate the discussion with stakeholders on treatment plans if required

Impact

• Assisted all stakeholders to understand their information assets and technology risks.
• Insights on regulations helped the bank making cost-effective decisions
• Strong focus on adherence to budgeted spend has been observed when defining systems that require RTO of 4 hours
• Enabled the bank to report to MAS that it has completed its first round of assessments in a timely manner
• Provided an efficient approach that enables the bank to capture and address risks in a uniform manner
Case Studies – Offshore banking

The Global bank engaged PwC to perform an assessment to evaluate their global stance on Technology polices, procedures and controls adherence to APAC regulators, with over 72 issues for Singapore.

To address these issues, a MAS program was initiated and PwC were engaged to facilitate the remediation effort:

- understanding the current prescriptive changes that can processed for a quick wins
- engaging stakeholders from business, to develop multiple plans to find cost effective solution to especially with global data centre’s hosting critical systems for Singapore

The MAS program provides a great opportunity to make policy changes and innovate with cost effect solutions already used elsewhere in the bank:

- PwC have developed a framework to adhere to future regulatory requirements
- Developed innovate solutions with the banks staff to save cost and become compliant
Appendix: Useful Resources
Useful Resources

The MAS TRM Notice:


Useful documents:

• Instructions on Incident Notification and Reporting to MAS
• Incident Report Template
• FAQs – Notice on Technology Risk Management Guidelines
• MAS TRM Guidelines

The documents above can be found by following the link below.

**Definition of Financial Institution**

Financial institution has the same meaning as in section 27A(6) of Monetary Authority of Singapore Act (Cap.186).

(a) any bank licensed under the Banking Act (Cap. 19);
(b) any finance company licensed under the Finance Companies Act (Cap. 108);
(c) any person that is approved as a financial institution under section 28; [13/2007 wef 30/06/2007]
(d) any money-changer licensed to conduct money-changing business, or any remitter licensed to conduct remittance business, under the Money-changing and Remittance Businesses Act (Cap. 187);
(e) any insurer registered or regulated under the Insurance Act (Cap. 142);
(f) any insurance intermediary registered or regulated under the Insurance Act;
(g) any licensed financial adviser under the Financial Advisers Act (Cap. 110);
(h) any approved holding company, securities exchange, futures exchange, recognised market operator, designated clearing house or holder of a capital markets services license under the Securities and Futures Act (Cap. 289);
(i) any trustee for a collective investment scheme authorised under section 286 of the Securities and Futures Act, that is approved under that Act;
(j) any trustee-manager of a business trust that is registered under the Business Trusts Act (Cap. 31A);
(k) any licensed trust company under the Trust Companies Act (Cap. 336);
(ka) any holder of a stored value facility under the Payment Systems (Oversight) Act (Cap. 222A); and [42/2007 wef 01/11/2007]
(l) any other person licensed, approved, registered or regulated by the Authority under any written law, but does not include such person or class of persons as the Authority may, by regulations made under this section, prescribe.
Focus on risk, compliance will follow

Contact us

Tan Shong Ye  shong.ye.tan@sg.pwc.com  +65 6236 3262
Mark Jansen  mark.jansen@sg.pwc.com  +65 6236 7388
Manish Chawda  manish.chawda@sg.pwc.com  +65 6236 7447

This presentation has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2013 PricewaterhouseCoopers Limited. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers Limited which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.