**Contents**

[1. Risk Assessment Initiation Pack 1](#_Toc434854501)

[2. MAS TRM Notice 127 2](#_Toc434854502)

[3. MAS TRM Requirements 2](#_Toc434854503)

[4. Outsourcing Checklists 3](#_Toc434854504)

[5. Protection of Confidential Data 3](#_Toc434854505)

[6. Data Migration and Deletion at Contract Termination (Legally Enforced) 4](#_Toc434854506)

[7. Source Code Escrow (Legally Enforced) 4](#_Toc434854507)

[8. Penetration Testing for Internet Facing Systems 4](#_Toc434854508)

[9. Multi-Factor Authentication for Privileged Access and Access over the Internet 5](#_Toc434854509)

[10. Source Code Review 5](#_Toc434854510)

[11. Service Provider’s IT Controls related Policies and Standards 5](#_Toc434854511)

[12. Service Provider’s Independent Audit Reports 6](#_Toc434854512)

[13. Service Provider’s Data Centre TVRA 6](#_Toc434854513)

|  |
| --- |
| Risk Assessment Initiation Pack |
| **Requirement / Area of Assessment**: |
| * IT and Business Project Team Structure (IT Project Manager, IT Custodian, Business Project Manager, Business Owner). * Timesheet Project Code. * Detailed Application Functionality. * Application Data Flow, Data Processing and Connectivity. * Internet Facing? Penetration Testing and VA by The Company’s appointed Pen Tester. Vendor should agree in writing to this. This is done as part of meeting local regulatory requirements. * Is the Application identified as MAS-Critical? * Does the Application hold Customer PII? * Load Testing should be performed to ensure that the availability requirements of the Company are met. * Application Business Criticality * Is this Outsourcing? Is this Cloud Computing? Is this Material Outsourcing? * What hardware and software stack are necessary to enable the service? Does the hardware and software align to The Company’s IT Architecture Recommendations? * Vendor access to The Company’s Systems? Long-standing access should not be allowed. Vendor should be onsite and The Company’s IT Infra/Support staff will perform implementation. Or a Webex session should be setup so that The Company’s IT infra/Support staff can monitor the implementation. |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| MAS TRM Notice 127 |
| **Requirement / Area of Assessment**: |
| <http://www.mas.gov.sg/~/media/resource/legislation_guidelines/insurance/notices/Notice%20MAS%20127.pdf>  Is the Application identified as MAS-Critical?  Does the Application hold Customer PII?  1-hour Notification Channel should be established.  High-Availability for MAS-Critical Systems. |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| MAS TRM Requirements |
| **Requirement / Area of Assessment**: |
| MAS TRM Checklist:  <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM_Checklist.xlsm>  MAS TRM Guidelines:  <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf> |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Outsourcing Checklists |
| **Requirement / Area of Assessment**: |
| Material outsourcing arrangement is where any of the following circumstances apply:   * A defect or failure in the performance of the outsourcing activity would significantly impair:  1. The company’s continuing compliance with regulatory or statutory requirements; 2. The company’s financial performance or its continuing ability to conduct its business; 3. The soundness or continuity of the company’s services or activities; or 4. The company’s ability to service its customers in a timely and appropriate way.   For Material Outsourcing, MAS should be notified about the Outsourcing.  *The Company’s Outsourcing Due Diligence Checklist* document should be filled.  MAS Outsourcing Technology Questionnaire:  <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TQoutsourcing.doc>  New: <http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Technology%20Questionnaire%20for%20Outsourcing%202015.docx> |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Protection of Confidential Data |
| **Requirement / Area of Assessment**: |
| Confidential data should be protected through Encryption at Rest, In-Motion and At Endpoints (Hard Disk Encryption; Data Loss Prevention – Internet Access, Email, Instant Messaging, Printing, Portable Devices). |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Data Migration and Deletion at Contract Termination (Legally Enforced) |
| **Requirement / Area of Assessment**: |
| All Company data held by the Service Provider and its Sub-Service Providers in any media format (Storage Disks, Storage Tapes, and Printed Papers) should be migrated to The Company’s systems and securely deleted / destroyed from the Service Provider’s systems, once the contract between The Company’s and the Service Provider ceases or when a demand has been made by The Company’s for the secure deletion of its data.  How would this be possible if logical-data-comingling exist? How would this be managed for comingled data in tape backups? |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Source Code Escrow (Legally Enforced) |
| **Requirement / Area of Assessment**: |
| Source code of the application should be deposited with an Escrow body, in case the vendor company goes out of business. |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Penetration Testing for Internet Facing Systems |
| **Requirement / Area of Assessment**: |
| The Company’s approved Penetration Testers should be used to test the services offered to The Company. Penetration Testing should be conducted in Production Network and Pre-Production/UAT Application Environment. Authenticated Penetration Testing should be conducted in the Application Environment, instead of a Black Box testing. |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Multi-Factor Authentication for Privileged Access and Access over the Internet |
| **Requirement / Area of Assessment**: |
| Multi-Factor Authentication should be used for Privileged Access to The Company’s Confidential Data / The Company’s Service Administration. |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Source Code Review |
| **Requirement / Area of Assessment**: |
| Source Code Review should be performed for Critical Code Modules (Authentication, Authorization, Transaction) |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Service Provider’s IT Controls related Policies and Standards |
| **Requirement / Area of Assessment**: |
| Please provide Service Provider’s IT Controls related Policies and Standards |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Service Provider’s Independent Audit Reports |
| **Requirement / Area of Assessment**: |
| Please provide Service Provider’s Independent Audit Reports – ISO 27001, ISO 27002, SOC 1, SOC 2 |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |

|  |
| --- |
| Service Provider’s Data Centre TVRA |
| **Requirement / Area of Assessment**: |
| Please provide Service Provider’s Data Centre – Threat and Vulnerability Risk Assessment (TVRA) |
| **IT Security – Review / Comments:** |
|  |
| **3) Potential and Confirmed Risks:** |
|  |