Risk Maturity Assessment Guide

High-level control objectives
<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Modification</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014/08/18</td>
<td>1.0</td>
<td>Initial Release</td>
<td>Marco Gunther</td>
</tr>
</tbody>
</table>
# Contents

1. Risk Management ................................................................................................................. 4
2. Information Security - Policies, Standards and Risk Management Structure .................. 4
3. Organization .............................................................................................................................. 5
4. Incident Management and Disaster Recovery ................................................................. 6
5. Information Technology Environment ............................................................................... 6
6. Business Practices .................................................................................................................... 8
1. RISK MANAGEMENT

Ogloba has ensured that a risk management program has been established to proactively assess risks to information, facilities and other resources (e.g. media, documentation, and so on) related to services provided to its clients. The risk management program has an assigned owner in every Local Country Office (LCO) and is periodically updated to include the latest threat scenarios.

The Ogloba LCO team conducts a regularly scheduled annual risk and control assessment (with internal and external audits when appropriate).

Results from the most recent risk assessment(s) and/or Internal Audit reports are available on demand, including a documented risk assessment program allowing proactive management of data sharing and non-data sharing risks. A periodic execution of the risk assessment program is performed to include current threats and vulnerabilities. Potential areas of consideration for the risk program include the following components:

- Governance plan
- Program owner
- Policy and procedures
- Range of business assets to be evaluated (People, Process, Technology and Data)
- Range of Threats (risks)
- Risk Scenarios - A distinction between Threats, Vulnerabilities and Impact to those assets
- Scoping and context (weighting of High, Medium, and Low risk areas)
- Training programs
- Risk evaluation criteria
- Control effectiveness criteria
- Level of ownership of business assessments

These are fully documented, and reviewed, assessed and approved annually. Please refer to the “Ogloba-GCS-Risk-Assessment-Instructions” document.

2. INFORMATION SECURITY - POLICIES, STANDARDS AND RISK MANAGEMENT STRUCTURE

Ogloba makes sure that relevant Policies and Standards exist in every LCO to protect client’s information, including at Third Party locations, as well as to examine the Risk Management Framework. This ensures a proactive and strong risk framework within a Third Party location to protect client’s information and delivery SLAs.

Ogloba has documented policies (including Information Security policies) and procedures (including procedures associated with its services). Electronic copies of policies, procedures and operations manual are available on demand.

Documented policies, procedures, and/or operations manuals for all services that are provided to clients are reviewed, approved prior to distribution, accessible, and published in a timely manner, including documented security policies covering different facets of information security. C-Suite members approve/endorse security policies, and the policies are reviewed and updated annually.
Documented policies allow employees and contractors to adopt consistent guidelines with regards to information and technology security.

Areas of inclusion in the security policy are:

- Organizational Security
- Asset Management
- Physical and environmental security
- Communications and Connectivity
- Change Control
- Data Integrity
- Incident Response
- Privacy
- Backup and Off-site Storage
- Vulnerability Monitoring
- Information Classification
- Data-handling policy
- Security configuration standards for networks, operating systems, applications and desktops

These are fully documented, and assessed, reviewed and approved yearly. Please refer to the “Information Security Policy” document.

3. ORGANIZATION

Ogloba ensures it has a formal, documented recruitment process. Staffing needs are reviewed, and agreed, by Local Country Office Managers, in consultation with Suite-C members.

Position roles and responsibilities are clearly defined. As part of the rigorous and structured recruitment process, potential candidates are assessed against core selection criteria to ensure their suitability to perform the role. Finalist candidates are screened before any final offer of employment is made. In addition, Ogloba has a policy of posting hire information, including non-selection reasons for each candidate, in an auditable record. The recruitment process cannot proceed to conclusion (i.e. formal appointment of the new staff member) until this has been completed.

Quarterly attrition rates are also documented.

Recruitment procedures are fully documented and regularly reviewed. Please refer to the “Hiring Process Book” document.

Ogloba ensures that there is a clearly defined organizational structure. It is Ogloba's intention to respect the current organizational chart, ensuring continuity in management, accountability, and output. This structured approach to recruitment and organization ensures that the overall quality of work carried out remains of the highest possible standard, in cases of increased workload demands.
4. INCIDENT MANAGEMENT AND DISASTER RECOVERY

Ogloba ensures it operates a formal, and documented, incident management procedure so that in the event of an incident, it can be dealt with in an effective and timely manner. Please refer to the “Incident Management” document.

The incident management policy and/or procedures includes the following attributes:

- Organizational structure is defined
- Response team is identified
- Response team availability is documented
- Timelines for incident detection and disclosure are documented
- Incident process life-cycle is defined, including the following discrete steps:
  1. Identification
  2. Assignment of severity of each incident
  3. Communication
  4. Resolution
  5. Training
  6. Reporting

To ensure continued business operation, that disasters can be recovered, and that risks of future incidents are minimized, Ogloba has in place a formal recovery process, outlining likely incident scenarios, and defining courses of remedial action. It is partially documented, and reviewed. Please refer to the “Disaster Recovery” document.

Ogloba has experienced incidents that resulted in adjustments to formal procedures. All such incidents are recorded, and subsequent actions documented in order to find permanent solutions and reduce the likelihood of similar incidents happening in future. Please refer to the incidents reports of last year, the “Incident Report-20131213.pdf” and “Incident Report-20131216.pdf” documents.

5. INFORMATION TECHNOLOGY ENVIRONMENT

Ogloba ensures that it operates in such a way that data security is paramount.

- The Data Center utilized by Ogloba has achieved BS7799 and ISO27001 standards for Information Security Management processes, and CMMI Level 3 for Quality processes, ensuring strong levels of security and environmental controls. Please refer to the “Introduction of Hosting” document.

- At a desktop control level, we have installed Avira Antivirus and Microsoft Security Essentials on every computer, and these are updated to the newest version every day. We use Google Apps (Gmail for Business) for our e-mail system, which prevents a lot of e-mail viruses.
- User Access Administration is carefully controlled. We operate under role-based user schemas, use a formal segregated user administration team, and perform regular recertification. We segregate User Access Administration from many groups.

- Our group classification depends on different areas, leaders, project teams, commercial teams, develop teams, IT teams, support teams and customers.

  When a new user needs to access a new operating system, application and/or infrastructure component, they need to ask their line manager, who then asks the system manager to grant the necessary permissions or create an account.

- Should an employee leave for any reason, their permissions and accounts are immediately suspended, and their successor takes over their job, documents, etc. using a new account. The account of the original employee is then deleted. In both scenarios, recertification of permissions and accounts will be initiated every 6 months.

- Ogloba operate managed servers with security tool-sets including:
  1. Monitoring tools to monitor the server capacity such as storage/memory usage, and inbound and outbound connection history.
  2. Scheduled automatic housekeeping tasks.
  3. Dedicated administrator role for accessing the server to undertake deployment, administration, and maintenance tasks.
  4. Daily backup of applications, and real time data synchronization of DB server from production to standby DB server.

- Ogloba's cyber/network controls operate via a single-tier, non-managed network. It uses a Firewall to filter unwanted flow. Please refer to the “Ogloba-Solution-Diagram” document.

- Remote Access Control is allowed for only a limited number of staff, and uses a Virtual Private Network (VPN) and multi-factor authentication. Overall, we have 5 levels of VPN for different purposes:
  1. (Level 1) For super administrators: allows access to every site and the management of every VPN account.
  2. (Level 2) For administrators: allows access to every site and the management of every VPN account except for super admin.
  3. (Level 3) For developers: allows access to their relevant formal sites and testing sites.
  4. (Level 4) For customer service staff: allows access to back offices.
  5. (Level 5) For users to have training and make presentations: allows access only to testing sites.

  All of these VPNs or accounts will be changed or deleted every 6 months, or whenever an employee leaves the company.

- Ogloba uses third party companies when required, subsequent to an informal/infrequent, though documented, risk assessment process. Please refer to the
Change Management is carried out according to a fully documented process, with changes authorised and independently approved. Our change procedure consists of three activities: initiation, review, and approval.

Change requests can be initiated by a customer, management staff, project sponsor or proposed by a user of the system.

All Change Request Forms must first be provided to the Project Manager.

All Project Change Request forms must be reviewed and approved by the Project Manager.

All change requests will be subject to Change Approval Criteria consisting of 4 levels: Critical, High, Medium, and Low.

Please refer to the “Change Management Procedure” document.

6. BUSINESS PRACTICES

The integrity and ethics of the Ogloba organization and employees is taken very seriously. All aspects of our business practices pertaining to gifts, complaints, and fraud are formally structured and fully documented. The gift prohibition policy is fully documented, reviewed, approved and implemented. Please refer to the “Anti-Bribery and Anti-Corruption Policy” document.

Fraud monitoring is subject to formal processes, procedures, and documentation of monitoring and communication. Please refer to the "Code of Business Conduct and Ethics" document.

The Ogloba complaints procedure is a fully documented process. Complaints are monitored and tracked to ensure issues are resolved in a timely manner. Complaints are communicated to the support team personnel, for which we have two processes:

1. First, we use JIRA, an online platform for users to build plans, assign work and track tasks. JIRA is used with our customers and internal members. Once someone creates an issue, selects the priority (level of importance), classifies it to relevant project groups and assigns it to the relevant people, the procedure starts. The relevant people will receive an e-mail notification for this issue and start to handle it immediately. After the issue has been resolved, and reviewed by original task creator, the procedure is closed.

2. Second, clients can also send e-mails to our hotline. Ogloba will receive a message (including via cellphone) and start to work on the issue immediately according to the SLA. Every issue from JIRA, and those e-mailed, will be saved and retained to support investigations in the future.