Executive Summary
Proposal to Implement Information Security Management System for our Organization

The purpose of this document is to propose the implementation of Information Security Management System (ISMS) for our organization. I, as the CISO, recommend to implement and manage ISMS in our organization to protect confidentiality, integrity and availability of our information assets.

Our organization has grown significantly through business acquisitions during the last 5 years. These acquisitions lack adequate controls over their information security. The implementation of ISMS will bring information security under firm management control, allowing direction and improvement where needed. Better information security will reduce the risk of incidents, incident-related losses and costs.

Criteria for information security risk reduction and providing a security baseline:
- Identify and mitigate the information security risks arising from our operational activities.
- Protect information assets against misuse, unauthorized access, or malicious attack.
- Apply the appropriate level of security to maintain the confidentiality, integrity, and availability of information assets across their lifecycle.
- Monitor, log, and report any actual or suspected data breaches.
- Protect the organization brand and reputation.
- Ensure that employee’s personal data is securely maintained and protected in accordance with privacy laws and regulations.

Course of action: The security policies shall be implemented and control objectives (criteria) achieved:
- Periodically assessing risks and planning their mitigation.
- Creating awareness of security policies & objectives among employees through security awareness training.
- Providing necessary resources, infrastructure and funds for implementing the security system.
- Auditing the security processes and procedures periodically.
- Adopting best practices in information security management by taking inputs from security standards.
- Ensuring implementation of security framework in accordance with policies and processes.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify &amp; mitigate information security risks</td>
<td>ISMS provide comprehensive, well-structured approach increasing the likelihood that all relevant information security threats, vulnerabilities and impacts will be identified, assessed and treated rationally.</td>
</tr>
<tr>
<td>Protect information assets</td>
<td>ISMS allow the organization to concentrate effort and resources on specific additional security requirements necessary to protect particular information assets.</td>
</tr>
<tr>
<td>Maintain confidentiality, integrity &amp; availability of information assets</td>
<td>ISMS shall be a part of the overall compliance framework, based on a business risk approach to establish, implement, operate, monitor, review and continuously improve security controls required to maintain the confidentiality, integrity, and availability of information assets.</td>
</tr>
<tr>
<td>Monitor &amp; report security breaches</td>
<td>ISMS shall enable the organization to manage its security risk exposure from the perspective of prevention, detection, containment and recovery.</td>
</tr>
</tbody>
</table>
**Protection of Employee Personal Data**: ISMS shall enable the organization’s information governance obligations to clients, potential clients, shareholders, investors, business partners and employees, the commitment to provide quality services while protecting their information assets.

**Protection of Organization Brand & Reputation**: ISMS is based on globally recognized and well-respected security standards and requirements of ISO 27001 & Sarbanes-Oxley Act.

**Alternative Option: Outsource Information Security to Managed Security Service Provider (MSSP)**

**Advantages:**
- **Cost Savings**: MSSP costs for analysts, security appliances/applications and facilities are distributed across their entire customer base.
- **Security Expertise**: MSSP have a dedicated team of security specialists to ensure our network is as protected as possible. They are also able to keep up with the latest security trends.
- **Customer Support**: MSSP generally provide real-time information security reporting 24 hours a day, 7 days a week, 365 days a year. This is critical for our organization because the timing of a cyber-attack is almost impossible to predict. We can set a service level agreement (SLA) for our exact needs and have the legal backing to have it guaranteed, giving us peace of mind regarding network protection.

**Disadvantages:**
- **Security Costs Not Completely Eliminated**: MSSP does not completely eliminate the security costs, for example, we will still need an in-house CISO for the MSSP to report to and coordinate with. MSSP offer security expertise but they are meant to supplement our own security team, not replace it.
- **Risk of Letting MSSP Handle Sensitive Information**: Allowing MSSP to handle personal identifiable information (PII) may not be acceptable to our organization due to legal and confidentiality issues in the case of a data breach. The accountability of the organization cannot be outsourced.
- **Lack of Management Control**: No guarantee of data protection, which leads to risk-related to lack of control. Outsourcing can introduce additional threats to the information security of our organization.
- **No Way to Ensure Effectiveness**: No visibility how MSSP handles updates, maintenance and trouble-shooting.

**Summary Analysis**
Our organization needs to take more active approach to managing information security risk. This requires the establishment of an effective governance structure for data security risk, risk assessments, control reviews, and remedial plans executed in a continuous cycle of improvement.

The ISMS will be a part of the overall compliance framework, based on a business risk approach to establish, implement, operate, monitor, review and continuously improve security controls required to maintain the confidentiality, integrity, and availability of information assets. The ISMS framework shall apply to all employees, contractors, vendors, in any location and all users of organization wide information assets. It is based on the requirements of ISO 27001 and Sarbanes-Oxley Act (SOX).

The Information security governance at the strategy layer cannot be outsourced because ultimate accountability always rests within the organization itself. The outsourcing of information security management in the tactical layer is the area where often the “gap” between strategy and operations (i.e. between the organization and the provider) can be found.

**Recommendation**
It is recommended to implement ISMS that optimally satisfies all objectives of our organization for information security and enhance our organization’s brand value and reputation.