**Word count**: 652 words (below the maximum of 660 words allowed, which is 600 + 10%).

Table of Contents

[Risk identification report 2](#_Toc116249468)

[1. Current risk assessment 2](#_Toc116249469)

[1.a. Methodology 2](#_Toc116249470)

[1.b. Threats and risks 2](#_Toc116249471)

[1.c. Potential mitigations 2](#_Toc116249472)

[2. Risk assessment of potential digitalisation 2](#_Toc116249473)

[2.a. Methodology 2](#_Toc116249474)

[2.b. Proposed changes 2](#_Toc116249475)

[2.c. Potential threats and risks 3](#_Toc116249476)

[2.d. Potential mitigations 3](#_Toc116249477)

[3. Recommendations 3](#_Toc116249478)

[3.a. Digitalisation 3](#_Toc116249479)

[3.b. Approach and timeline 3](#_Toc116249480)

[References 5](#_Toc116249481)

# Risk identification report

## 1. Current risk assessment

### 1.a. Methodology

* STRIDE model to qualitatively categorise security vulnerabilities (Jouini *et al*., 2014)
* DREAD model to quantify their business impact (Zhang *et al*., 2021)

### 1.b. Threats and risks

**Security risk**: very high (50.1/60).

* **S**poofing identity (DREAD score: 7.2):
  + Unencrypted emails with orders compromising clients’ **authentication** (Bhardwaj & Goundar, 2017).
* **T**ampering with data (DREAD score: 8.4):
  + Old computer with deliveries-related data jeopardising their **integrity** (Zhang *et al*., 2021).
* **R**epudation (DREAD score: 8.3):
  + The same wireless connection across corporate and personal devices **could** **expose** sensitive information (Talal *et al*., 2019).
* **I**nformation disclosure (DREAD score: 8.6):
  + Data **confidentiality** impacted by front desk’s computer’s unsecure storage (Bertino & Islam, 2017).
* **D**enial of service (DoS) (DREAD score: 8.7):
  + Comprised **availability** of two computers (Talal *et al*., 2019).
* **E**levation of privilege (DREAD score: 8.9):
  + Security breaches violating customers’ **authorisation**, thus ISO/IEC 27001:2005, GDPR and PCI-DSS (Mussmann *et al*., 2020).

### 1.c. Potential mitigations

* Using business email account and new computer (Bhardwaj & Goundar, 2017).
* Installing antivirus and anti-malware software, firewall, and the latest security patches on all devices, connected to virtual private network (VPN) (Harmening, 2017; Talal *et al*., 2019).
* Virtual private cloud (VPC) to back up data (Dhaya *et al*., 2021).

## 2. Risk assessment of potential digitalisation

### 2.a. Methodology

1. NIST CSF framework (Almuhammadi & Alsaleh, 2017) accounting for assets, business environment, governance, and supply chain.
2. Framework of Kovaitė & Stankevičienė (2019) considering competence, behavioural, and financial risks.

### 2.b. Proposed changes

* Via a third party:
  + Establishing data governance and designing a secure data and software architecture (Attard & Brennan, 2018).
  + Developing an e-commerce website with blog posts and a customer relationship management (CRM) tool, and social media for targeted marketing (Yadav & Rahman, 2017).

### 2.c. Potential threats and risks

* Financial risk: expensive third-party contractors (Attard & Brennan, 2018).
* Technical and data security risks in outsourcing the website development and using partial geo-location data from CRM for marketing (Almuhammadi & Alsaleh, 2017).
* Behavioural, competence-, and business environment-related risks in advertisements diluting the brand on social media (Kovaitė & Stankevičienė, 2019).

### 2.d. Potential mitigations

* Liaising with the local council to hire cheaper security experts (Almuhammadi & Alsaleh, 2017).
* Leveraging third-party company specialised in web development (Attard & Brennan, 2018), and geo-location and demographics data from social media posts (Yadav & Rahman, 2017).
* A social media marketer to enhance relevant customer reach (Zhang *et al*., 2021).

## 3. Recommendations

### 3.a. Digitalisation

1. For enhanced security:
   1. Business email account and industry-grade payment solution, e.g., PayPal (Bhardwaj & Goundar, 2017)
   2. CRM tool (Le Tan & Dai Trang, 2017)
   3. Corporate VPN and multi-factor authentication (Harmening, 2017)
   4. Third-party company to regularly perform security scans and penetration testing (Mussman *et al*., 2020)
   5. Required technical resources (Kovaitė & Stankevičienė, 2019) as per section 2.d
   6. HTTPS and the transport layer security to transfer sensitive information on the website in encrypted form (Harmening, 2017).
   7. VPC to back up and store data as encrypted (Dhaya *et al*., 2021).
2. To defend against malicious software, on all devices (Talal *et al*., 2019):
   1. Anti-virus and anti-malware software
   2. Firewall
   3. The latest security patches.
3. Changing passwords every 90 days and security training (Kovaitė & Stankevičienė, 2019).
4. Ensuring clients are aware of and agree with the company’s data privacy policy (Zhang *et al*., 2021).

### 3.b. Approach and timeline

Three-year-long and three-phase digital transformation (**Fig. 1**):

1. To achieve 50% growth:
   * data governance and security (Attard & Brennan, 2018),
   * online presence (Yadav & Rahman, 2017).
2. To reduce costs by 24%:
   * internationalising the supply chain (Yan *et al*., 2022), identifying cheaper suppliers overseas.
3. To drive further growth by 25%:
   * Leveraging omnichannel marketing, ensuring customer retention (Yadav & Rahman, 2017).

Chart, waterfall chart

Description automatically generated

**Figure 1**. Gantt chart of proposed digitalisation.

## References

Almuhammadi, S., & Alsaleh, M. (2017) Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)* 7(3): 51-62.

Attard, J., & Brennan, R. (2018) Challenges in value-driven data governance. In *OTM Confederated International Conferences “On the Move to Meaningful Internet Systems”*. 546-554. Springer, Cham.

Bertino, E., & Islam, N. (2017) Botnets and internet of things security. *Computer* 50(2): 76-79.

Bhardwaj, A., & Goundar, S. (2017) Security challenges for cloud-based email infrastructure. *Network Security* 2017(11): 8-15.

Dhaya, R., Kanthavel, R., & Venusamy, K. (2021) Dynamic secure and automated infrastructure for private cloud data center. *Annals of Operations Research* 1-21.

Harmening, J. T. (2017) Virtual private networks. In *Computer and Information Security Handbook*. Morgan Kaufmann. 843-856.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014) Classification of security threats in information systems. *Procedia Computer Science* 32: 489-496.

Kovaitė, K., & Stankevičienė, J. (2019) Risks of digitalisation of business models. In *Proceedings of 6th International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering 2019*.

Le Tan, T., & Dai Trang, D. T. (2017) Successful Factors of implementation Electronic Customer Relationship Management (e-CRM) on E-commerce company. *American Journal of Software Engineering and Applications* 6(5): 121-127.

Mussmann, A., Brunner, M., & Breu, R. (2020) Mapping the State of Security Standards Mappings. In *Wirtschaftsinformatik (zentrale tracks)*, 1309-1324.

Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Alsalem, M. A., Albahri, A. S., ... & Alaa, M. (2019) Comprehensive review and analysis of anti-malware apps for smartphones. *Telecommunication Systems* 72(2): 285-337.

Yadav, M., & Rahman, Z. (2017) Measuring consumer perception of social media marketing activities in e-commerce industry: Scale development & validation. *Telematics and Informatics* 34(7): 1294-1307.

Yan, Z., Lu, X., Chen, Y., & Wang, K. (2022) Institutional distance, internationalization speed and cross-border e-commerce platform utilization. *Management Decision*.

Zhang, L., Taal, A., Cushing, R., de Laat, C., & Grosso, P. (2021) A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *International Journal of Information Security* 1-17.