Risk Identification Report

1. Methodology

A custom 5-step approach was employed to assess the risks related to the current and the future state of the Pampered Pets business:

Step 1. Identification of business objectives

Step 2. Visualisation of the business structure

Step 3. Analysis of potential threats by using STRIDE (Microsoft, 2009) and DREAD (Microsoft, 2009).

Step 4. Mapping the threats identified with business objectives

Step 5. Identification of mitigations and estimation of effort needed

It is believed that the custom 5-step approach is more suitable for three reasons: (1) The resulting report is much understandable by the stakeholders, and it is more suitable for small businesses than other business-oriented approaches like PASTA (UcedaVelez & Morana, 2015: 317-478). (2) By using STRIDE and DREAD together, risks can be enumerated in a quantitative manner. (3) It incorporates business objectives to the assessment process.

The following DREAD rating criteria was employed:

DREAD Rating Criteria	Threat rating		Risk rating	
	High	3	High	12-15
	Medium	2	Medium	8-11
	Low	1	Low	5-7

The MITRE ATT&CK (MITRE, 2022) library was used to enumerate the threats and to identify the mitigations. Threat (technique) and mitigation IDs were also included for reference.

2. Risk assessment of the current state of the business

2.1. Business objectives

2.1.1. Explicit objectives:

- Retain existing customer base (O11)

2.1.2. Implied objectives:

- Avoid disruptions in the business (O32)
- Maintain the quality of the products (O33)

2.2. Data flow diagram of the business

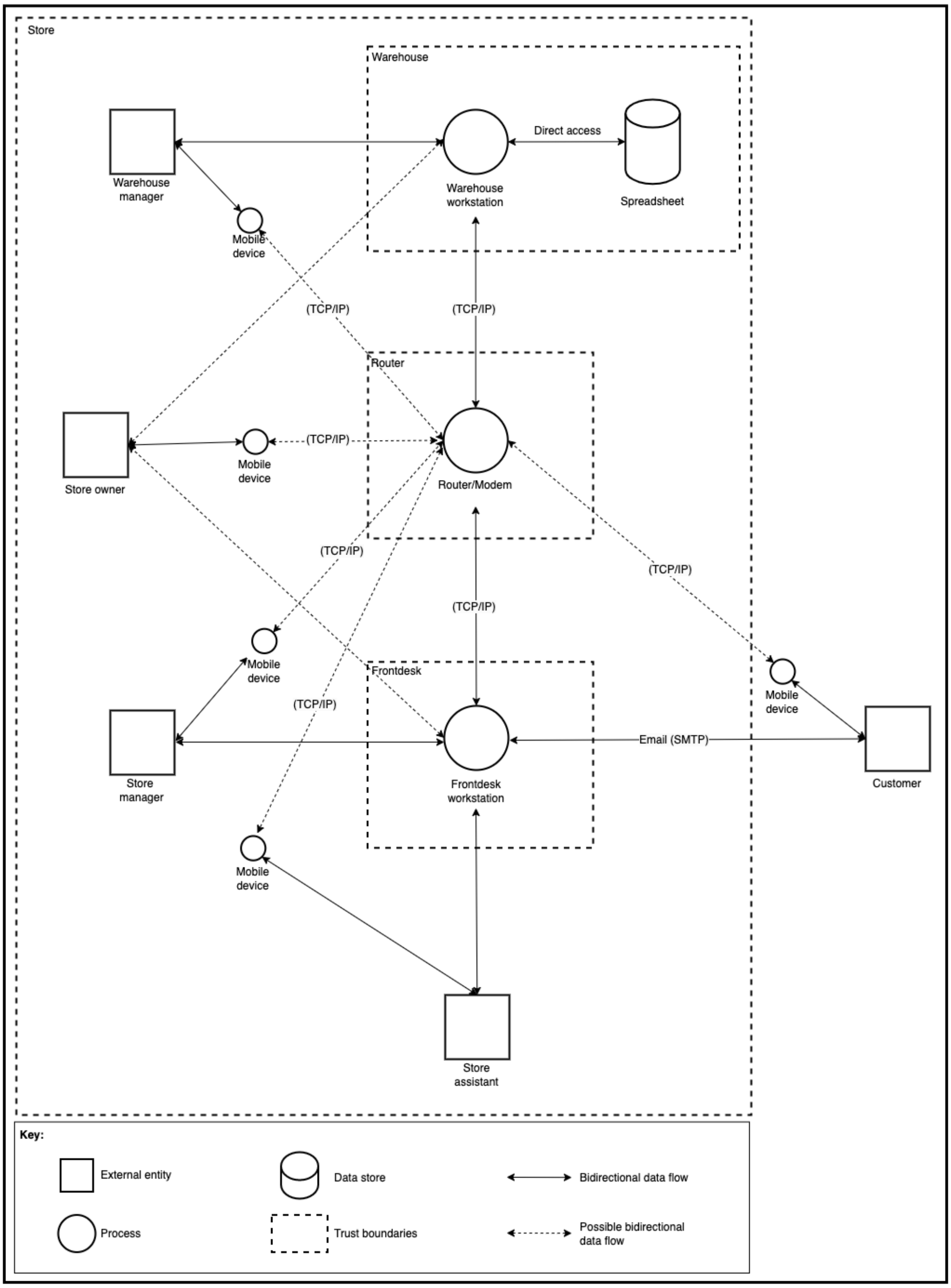
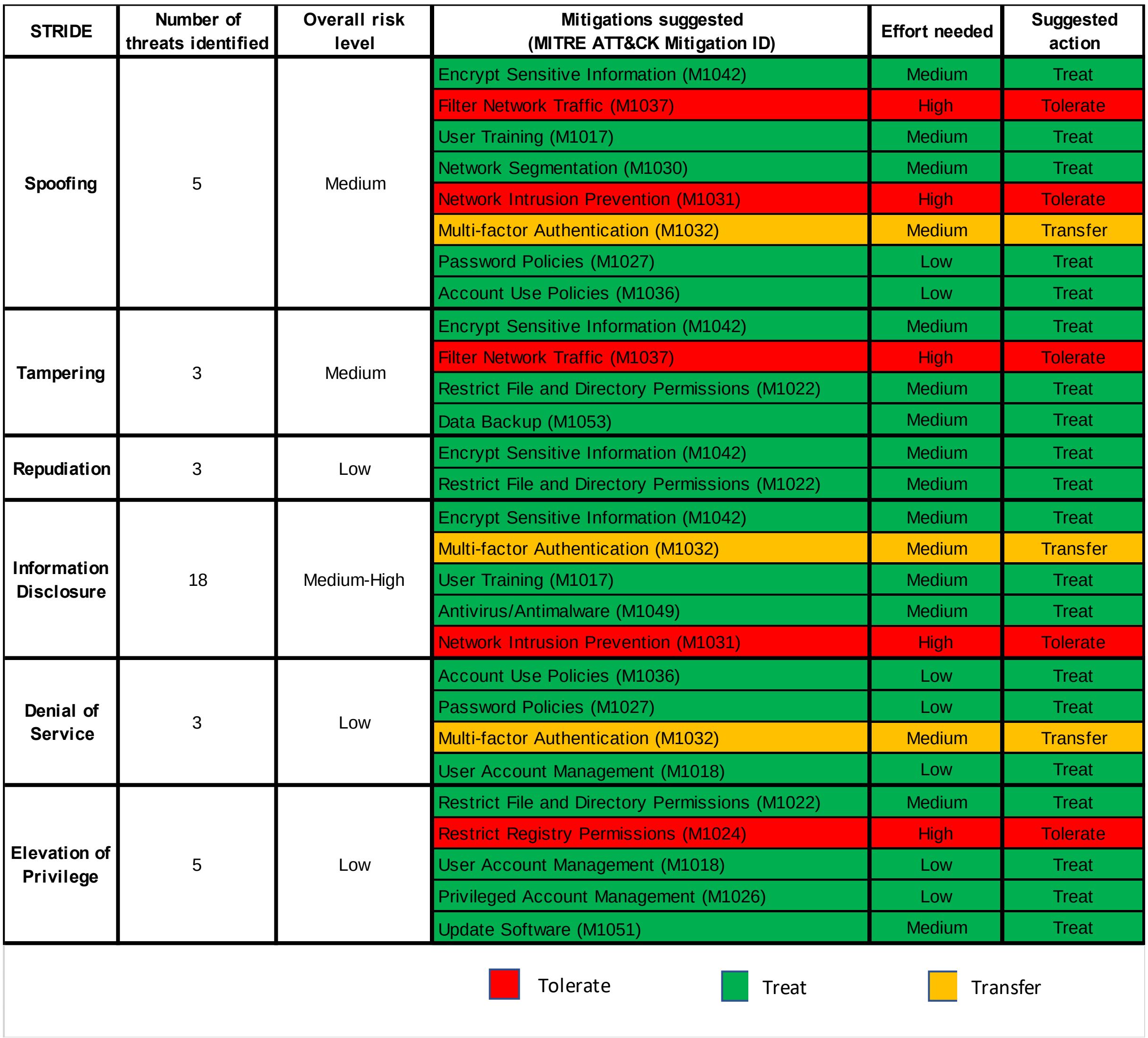


Diagram 1 - The data flow diagram of the current state of the Pampered Pets business

2.3. Enumeration of threats:

STRIDE	Threats Identified (MITRE ATT&CK ID)	D	R	E	A	D	Total DREAD Score	Risk	Related Business Objective
Spoofing	Adversary-in-the-Middle (T1557)	3	1	2	3	1	10	Medium	O32
	Brute Force (T1110)	3	1	2	1	1	8	Medium	O32
	OS Credential Dumping (T1003)	1	1	1	1	1	5	Low	O32
	Input Capture (T1056)	2	2	2	1	2	9	Medium	O32
	Modify Authentication Process (T1556)	2	1	1	1	2	7	Low	O32
Tampering	Data Manipulation (T1565)	3	2	2	3	1	11	Medium	O11,O32,O33
	Defacemenet (T1491)	2	1	1	1	1	5	Low	O11,O32
	Disk Wipe (T1561)	3	1	1	3	2	10	Medium	O11,O32,O33
Repudiation	Masquerading (T1036)	1	1	1	1	2	6	Low	O32
	Hide Artifacts (T1564)	1	1	1	1	3	7	Low	O32
	Indicator Removal (T1070)	1	1	1	1	2	6	Low	O32
Information Disclosure	Network Sniffing (T1040)	3	2	3	3	2	13	High	O32
	Active Scanning (T1595)	3	1	2	3	2	11	Medium	O32
	Account Discovery (T1087)	1	2	2	2	2	9	Medium	O32
	File and Directory Discovery (T1083)	1	2	2	2	2	9	Medium	O11,O32,O33
	Group Policy Discovery (T1615)	1	2	2	3	2	10	Medium	O32
	Network Service Discovery (T1046)	2	1	2	2	2	9	Medium	O32
	Password Policy Discovery (T1201)	3	2	2	3	2	12	High	O32
	System Information Discovery (T1082)	2	2	2	1	2	9	Medium	O32
	System Network Configuration Discovery (T1016)	2	2	2	1	2	9	Medium	O32
	Software Discovery (T1518)	2	2	2	1	2	9	Low	O32
	System Owner/User Discovery (T1033)	2	2	2	3	2	11	Medium	O32
	Email Collection (T1114)	3	2	2	2	2	11	Medium	O11,O32,O33
	Automatred Exfiltration (T1020)	3	1	1	1	1	7	Low	O11,O32,O33
	Gather Victim Identity Information (T1589)	3	3	3	1	2	12	High	O32
	Gather Victim Network Information (T1590)	3	3	3	2	2	13	High	O32
	Gather Victim Organisation Information (T1591)	3	3	3	3	2	14	High	O32
	Phishing (T1566)	3	2	2	1	1	9	Medium	O32
	Phishing for Information (T1598)	3	3	3	1	1	11	Medium	O11,O32,O33
Denial of Service	Resource Hijacking (T1496)	2	1	1	2	1	7	Low	O11,O32
	Brute Force (T1110)	3	1	2	3	1	10	Medium	O11,O32
	System Shutdown/Reboot (T1529)	1	2	2	1	1	7	Low	O11,O32
Elevation of Privilege	Abuse Elevation Control Mechanism (T1548)	1	1	1	1	1	5	Low	O32
	Boot or Logon Initialization Scripts (T1037)	2	1	1	1	2	7	Low	O32
	Scheduled Task/Job (T1053)	2	1	1	1	2	7	Low	O32
	Boot or Logon Autostart Execution (T1547)	2	1	1	1	2	7	Low	O32
	Exploitation for Credential Access (T1212)	2	1	2	2	1	8	Medium	O32

2.4. Suggested mitigations to the threats identified:



STRIDE	Number of threats identified	Overall risk level	Mitigations suggested (MITRE ATT&CK Mitigation ID)	Effort needed	Suggested action
Spoofing	5	Medium	Encrypt Sensitive Information (M1042)	Medium	Treat
			Filter Network Traffic (M1037)	High	Tolerate
			User Training (M1017)	Medium	Treat
			Network Segmentation (M1030)	Medium	Treat
			Network Intrusion Prevention (M1031)	High	Tolerate
			Multi-factor Authentication (M1032)	Medium	Transfer
			Password Policies (M1027)	Low	Treat
			Account Use Policies (M1036)	Low	Treat
Tampering	3	Medium	Encrypt Sensitive Information (M1042)	Medium	Treat
			Filter Network Traffic (M1037)	High	Tolerate
			Restrict File and Directory Permissions (M1022)	Medium	Treat
			Data Backup (M1053)	Medium	Treat
Repudiation	3	Low	Encrypt Sensitive Information (M1042)	Medium	Treat
			Restrict File and Directory Permissions (M1022)	Medium	Treat
Information Disclosure	18	Medium-High	Encrypt Sensitive Information (M1042)	Medium	Treat
			Multi-factor Authentication (M1032)	Medium	Transfer
			User Training (M1017)	Medium	Treat
			Antivirus/Antimalware (M1049)	Medium	Treat
			Network Intrusion Prevention (M1031)	High	Tolerate
Denial of Service	3	Low	Account Use Policies (M1036)	Low	Treat
			Password Policies (M1027)	Low	Treat
			Multi-factor Authentication (M1032)	Medium	Transfer
			User Account Management (M1018)	Low	Treat
Elevation of Privilege	5	Low	Restrict File and Directory Permissions (M1022)	Medium	Treat
			Restrict Registry Permissions (M1024)	High	Tolerate
			User Account Management (M1018)	Low	Treat
			Privileged Account Management (M1026)	Low	Treat
			Update Software (M1051)	Medium	Treat

🟥 Tolerate 🟩 Treat 🟨 Transfer

3. Risk assessment of the digitalised business

3.1. Business objectives

3.1.1. Explicit objectives:

- Grow the business by up to 50% by offering online services (O21)
- Reduce costs by up to 24% by changing to an international supply chain (O22)

3.1.2. Implied objectives:

- Avoid disruptions in the business (O32)
- Maintain the quality of the products (O33)

3.2. Data flow diagram of the digitalised business:

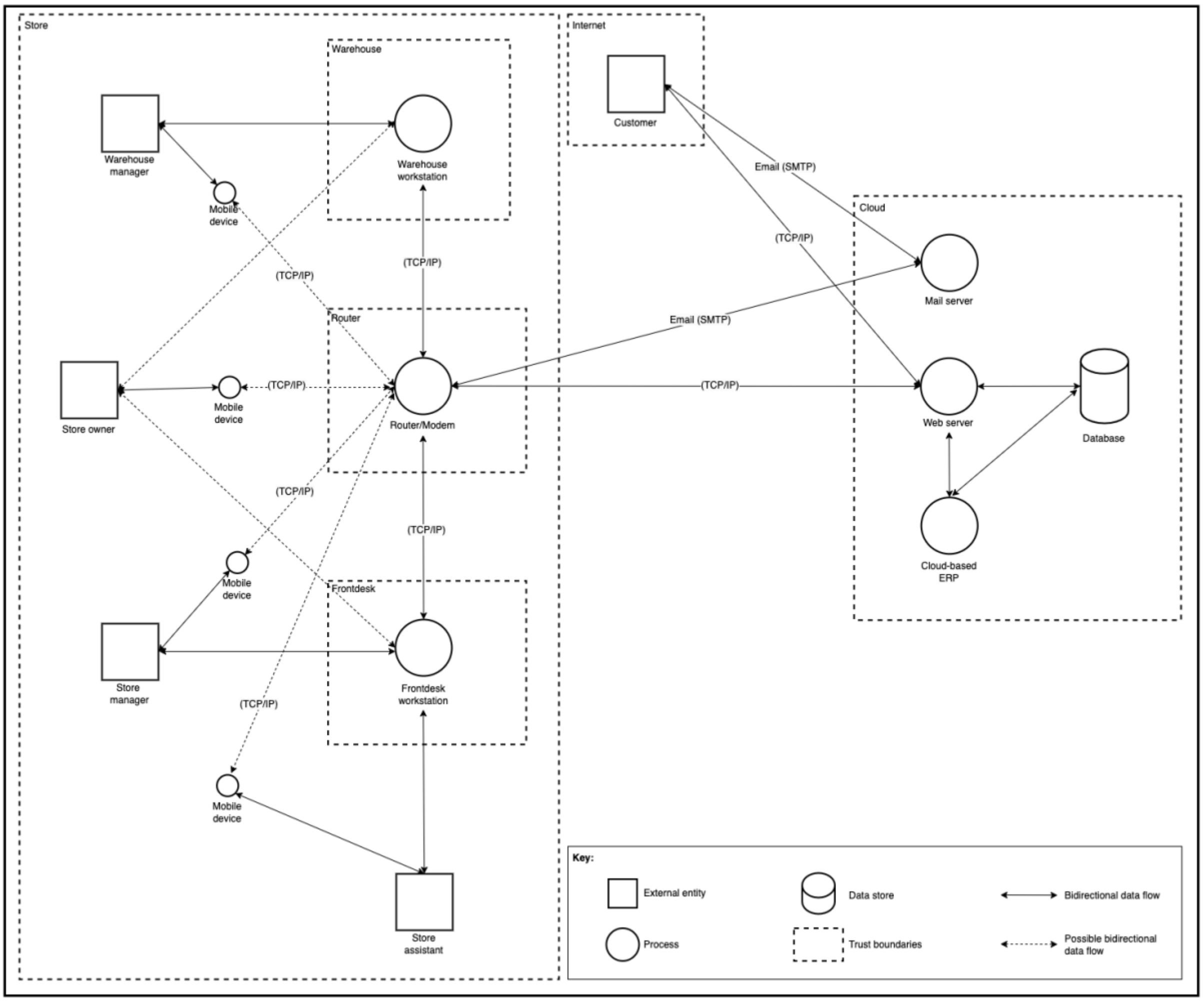


Diagram 2 - The data flow diagram of the digitalised Pampered Pets business

3.3. Suggested roadmap towards digitalisation of the business:

In order to conduct a successful digital transformation process, the following steps are recommended:

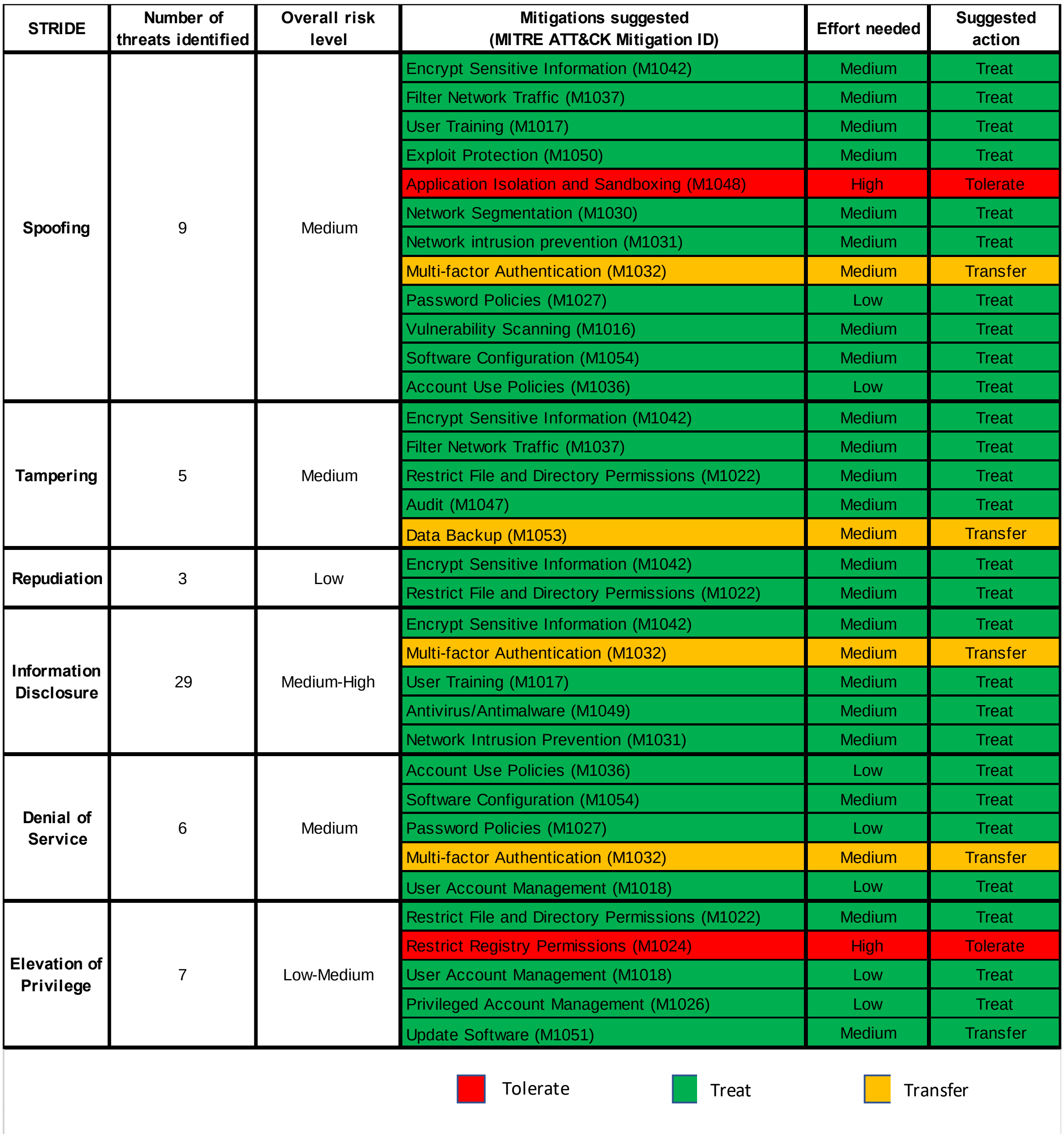
Recommendations	Justification
Set up an **e-commerce portal**	- Showcase company's products - Enable clients to submit orders
Set up/use an **Enterprise Resource Planning (ERP)** solution	- Track stocks, purchases and cashflow - Facilitate the switch to international supply chain (in line with business objectives)

Deploy/migrate to **cloud**	- Lower cost of ownership - Scale up and out when needed - Transfer some of the risks to cloud service provider
Launch **Search Engine Optimization (SEO)** campaign	- Improve search rankings - Drive organic traffic
Launch an **online marketing campaign** (incl. Social Media marketing)	- Increase brand awareness - Grow client base - Get/increase market share

3.4. Enumeration of threats:

STRIDE	Threats Identified (MITRE ATT&CK ID)	D	R	E	A	D	Total DREAD Score	Risk	Related Business Objective
Spoofing	Adversary-in-the-Middle (T1557)	3	1	2	3	1	10	Medium	O32
	Brute Force (T1110)	3	1	2	1	1	8	Medium	O21,O22,O32
	OS Credential Dumping (T1003)	1	1	1	1	1	5	Low	O32
	Input Capture (T1056)	2	2	2	1	2	9	Medium	O32
	Modify Authentication Process (T1556)	2	1	1	1	2	7	Low	O32
	Exploit Public-Facing Application (T1190)	3	2	2	3	2	12	High	O21,O32
	Forge Web Credentials (T1606)	2	1	1	1	2	7	Low	O21,O32
	Steal Web Session Cookie (T1539)	2	2	2	1	2	9	Medium	O21,O32
	Compromise Accounts (T1586)	2	1	1	1	2	7	Low	O21,O32
Tampering	Data Manipulation (T1565)	3	2	2	3	1	11	Medium	O32,O33
	Defacemenet (T1491)	2	1	1	1	1	5	Low	O21,O32
	Account Manipulation (T1098)	3	1	1	2	1	8	Medium	O32
	Modify Cloud Compute Infrastructure (T1578)	3	1	1	2	2	9	Medium	O21,O22,O32,O33
	Disk Wipe (T1561)	3	1	1	3	2	10	Medium	O32
Repudiation	Masquerading (T1036)	1	1	1	1	2	6	Low	O32
	Hide Artifacts (T1564)	1	1	1	1	3	7	Low	O32
	Indicator Removal (T1070)	1	1	1	1	2	6	Low	O32
Information Disclosure	Network Sniffing (T1040)	3	2	3	3	2	13	High	O32
	Active Scanning (T1595)	3	1	2	3	2	11	Medium	O32
	Account Discovery (T1087)	1	2	2	2	2	9	Medium	O32
	File and Directory Discovery (T1083)	1	2	2	2	2	9	Medium	O21,O32,O33
	Group Policy Discovery (T1615)	1	2	2	3	2	10	Medium	O32
	Network Service Discovery (T1046)	2	1	2	2	2	9	Medium	O32
	Password Policy Discovery (T1201)	3	2	2	3	2	12	High	O32
	System Information Discovery (T1082)	2	2	2	1	2	9	Medium	O32
	System Network Configuration Discovery (T1016)	2	2	2	1	2	9	Medium	O32
	Software Discovery (T1518)	2	2	2	1	2	9	Low	O32
	System Owner/User Discovery (T1033)	2	2	2	3	2	11	Medium	O32
	Cloud Infrastructure Discovery (T1580)	3	2	2	2	2	11	Medium	O21,O22,O32
	Cloud Service Dashboard (T1538)	3	2	2	3	2	12	High	O21,O22,O32
	Cloud Service Discovery (T1526)	3	2	2	2	2	11	Medium	O21,O22,O32
	Cloud Storage Object Discovery (T1619)	1	2	2	2	2	9	Medium	O21,O22,O32
	Credentials from Password Stores (T1555)	3	1	1	1	2	8	Medium	O21,O32
	Unsecured Credentials (T1552)	3	1	1	1	2	8	Medium	O32
	Email Collection (T1114)	3	2	2	2	2	11	Medium	O21,O22,O32,O33
	Automatred Exfiltration (T1020)	3	1	1	1	1	7	Low	O21,O32,O33
	Gather Victim Identity Information (T1589)	3	3	3	1	2	12	High	O32
	Gather Victim Network Information (T1590)	3	3	3	2	2	13	High	O32
	Gather Victim Organisation Information (T1591)	3	3	3	3	2	14	High	O32
	Search Open Technical Databases (T1596)	2	3	3	2	2	12	High	O21,O32
	Search Open Websites/Domains (T1593)	1	3	3	2	1	10	Medium	O21,O32
	Search Closed Sources (T1597)	1	3	3	2	1	10	Medium	O21,O32
	Search Victim-Owned Websites (T1594)	1	3	3	1	1	9	Medium	O21,O32
	Transfer Data to Cloud Account (T1537)	3	1	1	1	2	8	Medium	O21,O32
	Phishing (T1566)	3	2	2	1	1	9	Medium	O32
	Phishing for Information (T1598)	3	3	3	1	1	11	Medium	O32
Denial of Service	Resource Hijacking (T1496)	2	1	1	2	1	7	Low	O32
	Unused/Unsupported Cloud Regions (T1535)	2	1	1	2	1	7	Low	O21,O32
	Network Denial of Service (T1498)	3	2	3	3	1	12	High	O21,O22,O32
	Endpoint Denial of Service (T1499)	3	1	2	3	1	10	Medium	O21,O22,O32
	Brute Force (T1110)	3	1	2	3	1	10	Medium	O21,O22,O32
	System Shutdown/Reboot (T1529)	1	2	2	1	1	7	Low	O21,O22,O32
Elevation of Privilege	Abuse Elevation Control Mechanism (T1548)	1	1	1	1	1	5	Low	O32
	Boot or Logon Initialization Scripts (T1037)	2	1	1	1	2	7	Low	O32
	Scheduled Task/Job (T1053)	2	1	1	1	2	7	Low	O32
	Boot or Logon Autostart Execution (T1547)	2	1	1	1	2	7	Low	O32
	Valid Accounts (T1078)	3	1	2	2	1	9	Medium	O21,O22,O32
	Create Account (T1136)	3	1	2	2	1	9	Medium	O21,O22,O32
	Exploitation for Credential Access (T1212)	2	1	2	2	1	8	Medium	O21,O32

3.5. Suggested mitigations to the threats identified:



STRIDE	Number of threats identified	Overall risk level	Mitigations suggested (MITRE ATT&CK Mitigation ID)	Effort needed	Suggested action
Spoofing	9	Medium	Encrypt Sensitive Information (M1042)	Medium	Treat
			Filter Network Traffic (M1037)	Medium	Treat
			User Training (M1017)	Medium	Treat
			Exploit Protection (M1050)	Medium	Treat
			Application Isolation and Sandboxing (M1048)	High	Tolerate
			Network Segmentation (M1030)	Medium	Treat
			Network intrusion prevention (M1031)	Medium	Treat
			Multi-factor Authentication (M1032)	Medium	Transfer
			Password Policies (M1027)	Low	Treat
			Vulnerability Scanning (M1016)	Medium	Treat
			Software Configuration (M1054)	Medium	Treat
			Account Use Policies (M1036)	Low	Treat
Tampering	5	Medium	Encrypt Sensitive Information (M1042)	Medium	Treat
			Filter Network Traffic (M1037)	Medium	Treat
			Restrict File and Directory Permissions (M1022)	Medium	Treat
			Audit (M1047)	Medium	Treat
			Data Backup (M1053)	Medium	Transfer
Repudiation	3	Low	Encrypt Sensitive Information (M1042)	Medium	Treat
			Restrict File and Directory Permissions (M1022)	Medium	Treat
Information Disclosure	29	Medium-High	Encrypt Sensitive Information (M1042)	Medium	Treat
			Multi-factor Authentication (M1032)	Medium	Transfer
			User Training (M1017)	Medium	Treat
			Antivirus/Antimalware (M1049)	Medium	Treat
			Network Intrusion Prevention (M1031)	Medium	Treat
Denial of Service	6	Medium	Account Use Policies (M1036)	Low	Treat
			Software Configuration (M1054)	Medium	Treat
			Password Policies (M1027)	Low	Treat
			Multi-factor Authentication (M1032)	Medium	Transfer
			User Account Management (M1018)	Low	Treat
Elevation of Privilege	7	Low-Medium	Restrict File and Directory Permissions (M1022)	Medium	Treat
			Restrict Registry Permissions (M1024)	High	Tolerate
			User Account Management (M1018)	Low	Treat
			Privileged Account Management (M1026)	Low	Treat
			Update Software (M1051)	Medium	Transfer

🟥 Tolerate 🟩 Treat 🟨 Transfer

4. Summary and recommendations

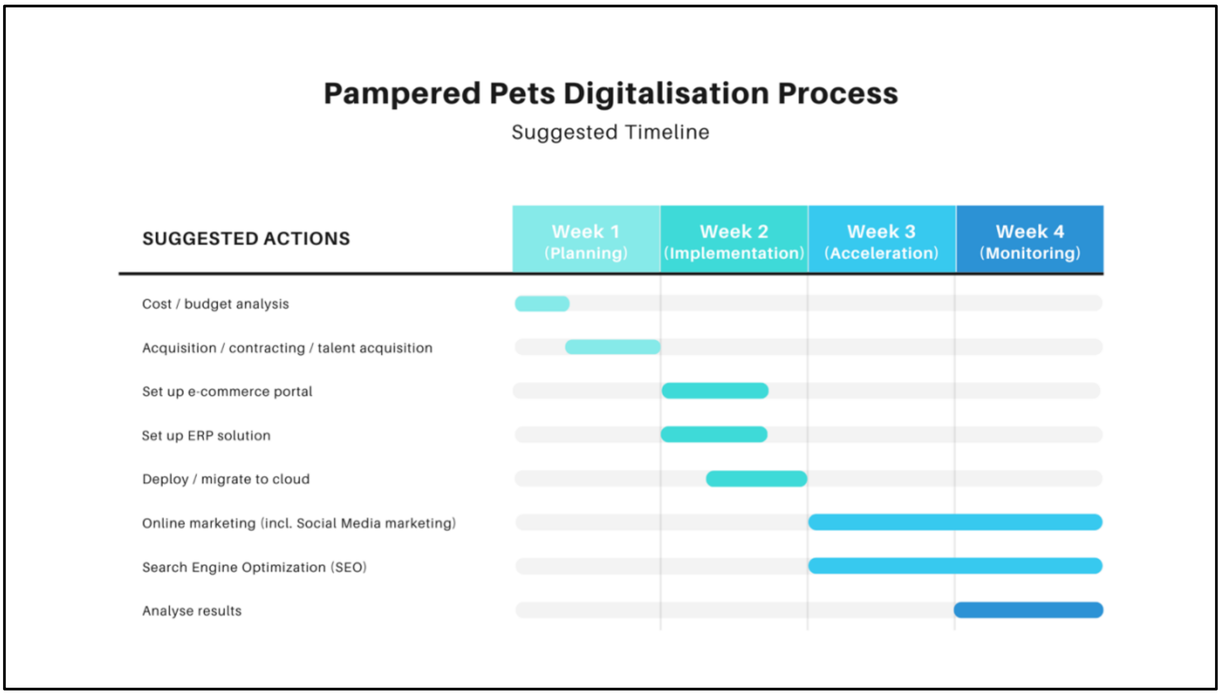
To reap the benefits of the latest technologies, Pampered Pets business is **advised to undergo a digitalisation process** in order to offer online services to its current and future clientele. Based on the findings discussed above, it is assessed that:

- An online presence could help Pampered Pets grow the business by 50%.

- It is highly likely that changing to an international supply chain via an ERP solution could reduce costs by up to 24%.
- If the digital transformation is not adopted by the business, it is highly likely that Pampered Pets will not be able to stand up to the competition and could lose up to 33% of its current clientele.

As can be seen from the risk assessment of the digitalisation scenario, the attack surface is significantly larger when using cloud services. Nevertheless, it is recommended to migrate and deploy the services to the cloud due to various benefits it offers as pointed out in section 3.3. It may also help secure the business effortlessly and efficiently by leveraging cloud-based services (e.g., automated backups, IDS, WAF).

The following timeline is suggested to put the recommendations mentioned in section 3.3 into practice:



Finally, qualitative risks such as non-compliance to standards such as GDPR (Data Protection Act, 2018) and PCI DSS (PCI SSC, 2022) should not be overlooked during the digitalisation process.

References:

Data Protection Act 2018, United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed 26 March 2023].

Microsoft (2009) The STRIDE Threat Model. Available from: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN [Accessed 26 March 2023].

Microsoft (2023) Threat modeling for drivers. Available from: https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers [Accessed 26 March 2023].

MITRE (2022) MITRE ATT&CK. Available from: https://attack.mitre.org [Accessed 26 March 2023].

PCI Security Standards Council (2022) PCI DSS v4.0 Quick Reference Guide. Available from: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf [Accessed 25 February 2023].

UcedaVelez, T. & Morana, M. M. (2015) *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. New Jersey: Wiley Publishing.