Risk Identification Report

“Pampered Pets”

1. Introduction

Pampered Pets, A high quality pet food store that employes 4 staff members and is operating through in-store sales. Cathey, the store manager, seeks to investigate an internet-based growth opportunity, online presence and its potential threats. This report aims to analyze the current and future state of their business model.

2. Methodology of Risk Assessment

ISO 31000 risk management Framework provides a comprehensive approach to assess risks related to digital transformation and proposes the following methods (Lalonde & Boiral, 2012):

1. **Risk Identification**

   Encourages the process of identifying risks both external and internal, this is critical as the business will undergo an online expansion and supply chain changes.

2. **Risk Assessment**

   In this instance, **STRIDE** and **OCTAVE** threat modelling approaches will be deployed to evaluate the current business model as well as the potential impact of transitioning to an online presence. Additionally, **OCTAVE** focuses on managing information related to information security risks within an

operational environment (Khan, et al., 2017). This aims to provide a fixable approach in identifying potential Risks.

3. **Risk Mitigation**

   This enables Pampered Pets to initiate required protocols against prioritized risks, allocate resources effectively, and accordingly with their business needs.

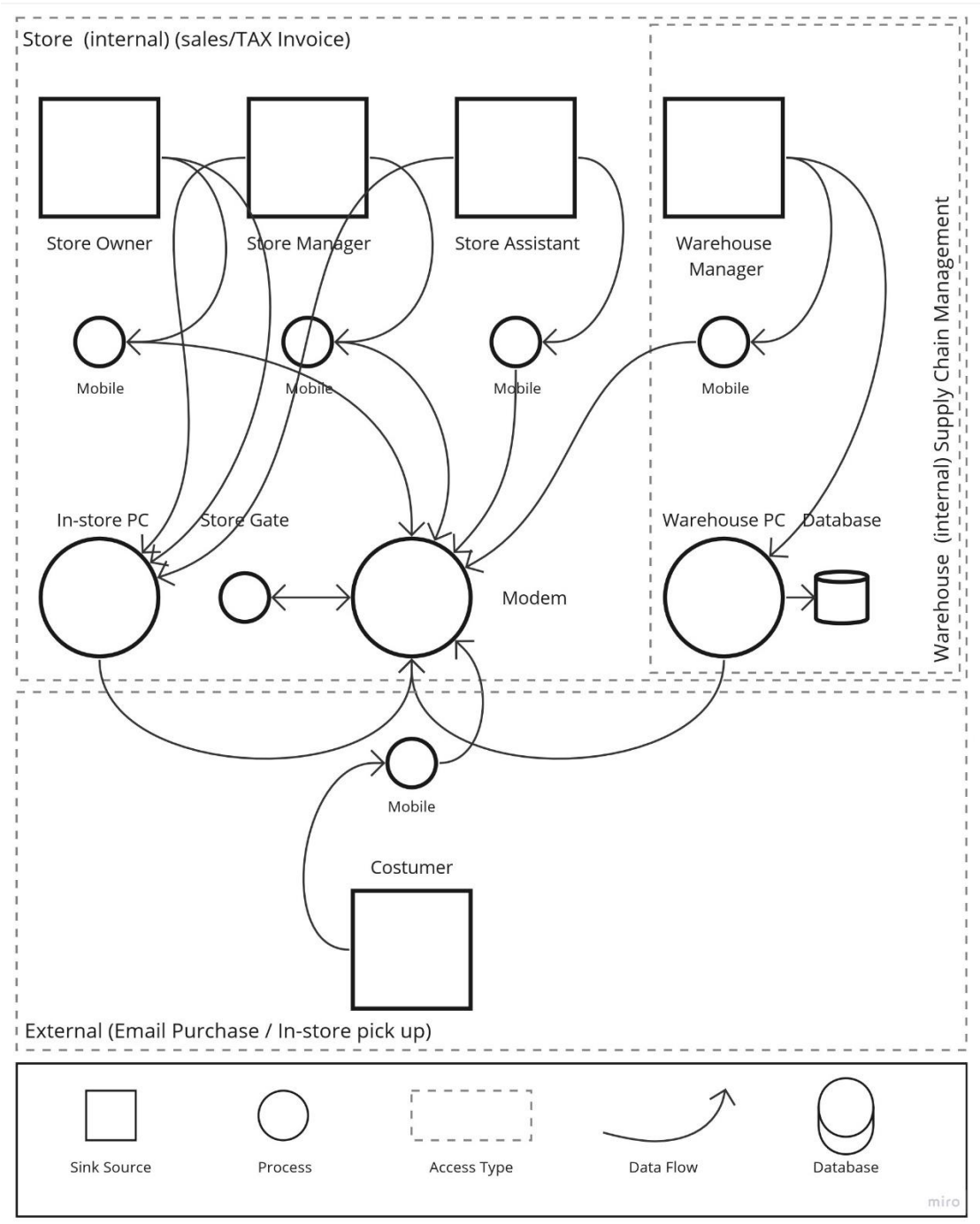
Given the unique aspects of pampered pets, ISO 31000 farmwork offers an adaptable and systemic approach that integrates with the business's objectives. As such, stakeholders are provided with a comprehensive and accurate risk assessment. In addition, the STRIDE model covers and array of potential threats ensuring a structured analysis, prioritization, and informed decision making (Mircosoft, 2009).

3. Section A: Current Business State

Current Business Objectives:

a. Maintain high quality ingredients.
b. Customer retention.
c. Effective operations.

Current Data Flow /IT Infrastructure:



Threat Modeling (Risk Identification & Mitigation):

CAPEC (Common Attack Pattern Enumeration and Classification) is a Library of common threats containing a detailed description of each threat and its attack patterns. This will be used to identify the risks associated with Pampered Pet's current business model (Yuan, et al., 2014).

STRIDE THREAT MODEL (RISK IDENTIFICATION)				
Threat Type	**Description of Threat**	**CAPEC ID**	**Potential Risks**	**Risk Level**
Spoofing	Impersonation of users/systems	CAPEC-66	Unauthorized access, data breach	High
	Unauthorized data access		Unauthorized data access, data exposure	High
Tampering	Unauthorized data modification	CAPEC-242	Data manipulation, inventory errors	High
	Unauthorized transaction modification		Transaction fraud, financial losses	High
Repudiation	Denying actions/transactions	CAPEC-114	Disputes, legal issues	Medium
	Falsifying evidence		False claims, accountability issues	Medium
Information Disclosure	Unauthorized data access	CAPEC-200	Data exposure, privacy violations	High
	Information leakage		Proprietary information loss	High
Denial of Service	System unavailability	CAPEC-26	Customer dissatisfaction, revenue loss	Medium
	Network resource exhaustion		Business disruption, service degradation	Medium
Elevation of Privilege	Unauthorized privilege escalation	CAPEC-32	Unauthorized access, data breach	High
	Unauthorized access to admin functions		Unauthorized control	High

STRIDE THREAT MODEL (RISK Mitigation)				
Threat Type	**Description of Threat**	**Mitigations**	**Priority**	**Action Needed**
Spoofing	Impersonation of users/systems	Implement strong multi-factor authentication for employees and customers. Regularly review access logs.	High	Transfer
	Unauthorized data access	Implement user role-based access controls and regular access reviews. Encrypt sensitive data.	High	Treat
Tampering	Unauthorized data modification	Implement data integrity checks and digital signatures. Use secure hashing algorithms.	High	Treat
	Unauthorized transaction modification	Implement tamper-evident transaction logs.	High	Treat
Repudiation	Denying actions/transactions	Implement comprehensive transaction logging and digital signatures.	Medium	Treat
	Falsifying evidence	Use immutable audit logs and timestamps.	Medium	Treat
Information Disclosure	Unauthorized data access	Implement strong access controls and encryption. Regularly audit access logs.	High	Treat
	Information leakage	Implement data loss prevention solutions.	High	Treat
Denial of Service	System unavailability	Implement load balancing, redundancy, and DDoS protection measures.	Medium	Treat
	Network resource exhaustion	Monitor network traffic for resource exhaustion patterns.	Medium	Treat
Elevation of Privilege	Unauthorized privilege escalation	Enforce least privilege principle. Use strong authentication and authorization mechanisms.	High	Treat
	Unauthorized access to admin functions	Implement strict access controls and regular security audits.	High	Treat

4. Section B: Future Business State

Future Business Objectives:

a. Online presence. (Potential growth of business up to 50%).
b. 24% cost reduction on supply chain. (Migration to international supply chain)
c. Customer retention. (Potential loss of clients up to 33% in the absence of online features)

Proposed Digitization Criteria:

d. <u>E-commerce.</u>
    i. Expandability, broader reach, and increased audience base
    ii. Convince, customer engagement, 24/7 Accessibility.
    iii. Increase in product range and detailed information.
    iv. Reduced risk of audience loss.
    v. Data insight on consumer behavior and sales preferences.

e. <u>Digital Marketing.</u>
    i. Social media engagement for encouraging brand loyalty and user-generated content.
    ii. Targeted advertising for Pampered Pet's specific audience and broader demographics.
    iii. Insured rapid growth.

iv. Search Engine Optimization (SEO) for organic traffic to Pampered Pet's e-commerce website.

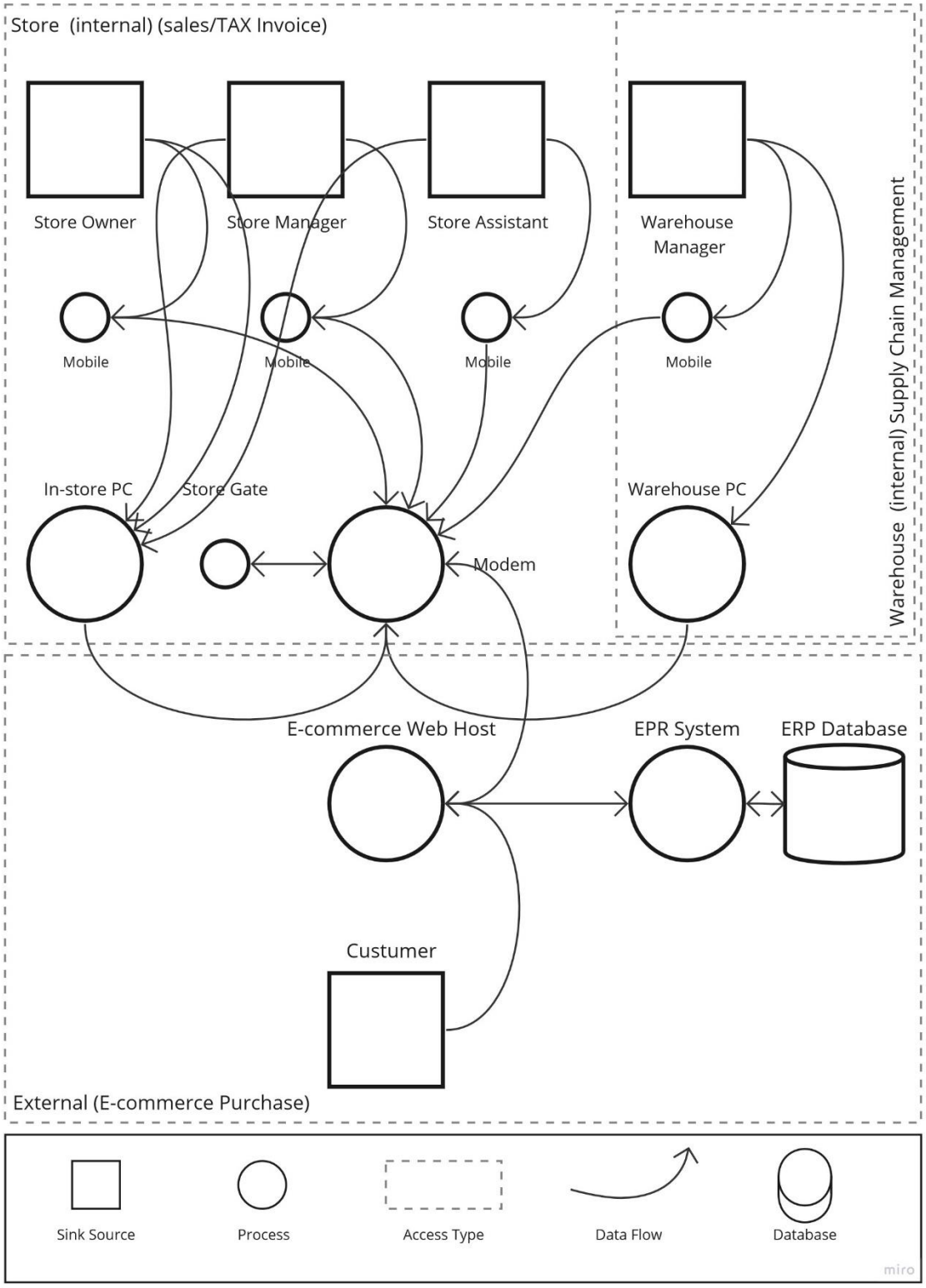
f. ERP Systems.

i. Inventory and order Processing, stockouts are prevented.

ii. Supplier management and efficient integration encourages diversity in suppliers and cost-efficient products.

iii. Order tracking and financial management.

Estimated Data Flow / Integration:



Threat Modeling (Risk Identification & Mitigation):

STRIDE / OCTAVE THREAT MODEL (RISK IDENTIFICATION)						
Threat Category	**Threat Description**	**CAPEC ID**	**Impact**	**Vulnerabilities**	**Safeguards**	**Risk Level**
Spoofing	Unauthorized access to digital systems	CAPEC-165	Loss of data integrity, unauthorized transactions	Weak authentication, compromised credentials	Strong authentication mechanisms, multi-factor authentication	High
	Impersonation of legitimate users	CAPEC-121	Unauthorized data access, unauthorized actions	Stolen credentials, lack of user verification	User verification processes, continuous monitoring	Medium
	Falsifying digital identities	CAPEC-217	Fraudulent activities, reputational damage	Lack of identity verification, weak authorization	Identity verification, strong authorization protocols	Medium
Tampering	Unauthorized modification of data or software	CAPEC-136	Data corruption, incorrect orders	Insufficient data validation, lack of integrity checks	Data validation, cryptographic signatures	High
	Altering product details	CAPEC-278	Customer dissatisfaction, revenue loss	Inadequate product data validation, weak access controls	Product data validation, strict access controls	Medium
	Modifying order information	CAPEC-167	Financial loss, operational disruption	Insecure data transmission, lack of order validation	Secure data transmission, robust order validation	Medium
Repudiation	Denying performed actions	CAPEC-20	Disputes, legal issues	Inadequate transaction logging, lack of audit trail	Comprehensive logging, digital signatures	High
	False denial of orders	CAPEC-156	Disputes, customer dissatisfaction	Inadequate order tracking, absence of digital signatures	Order tracking, digital signatures	Medium
	Denying online transactions	CAPEC-150	Reputational damage, legal consequences	Weak transaction verification, lack of non-repudiation	Strong transaction verification, non-repudiation mechanisms	Medium
Information Disclosure	Unauthorized access to sensitive information	CAPEC-215	Privacy breaches, data leakage	Insufficient access controls, weak encryption	Role-based access control, strong encryption	High
	Exposure of customer data	CAPEC-115	Privacy violations, legal penalties	Insecure data storage, lack of encryption	Secure data storage, encryption at rest	Medium
	Leaking business strategies	CAPEC-87	Competitor advantage, brand damage	Inadequate access control to strategic documents	Restrict access to sensitive documents, NDAs	Medium
Denial of Service	Disrupting digital services	CAPEC-79	Business downtime, loss of revenue	Network vulnerabilities, resource exhaustion	DDoS protection, redundant systems	High
	Network congestion attacks	CAPEC-99	Service disruption, customer frustration	Inadequate network monitoring, lack of traffic analysis	Network monitoring, traffic analysis	Medium
	Application-level floods	CAPEC-89	Application unavailability, diminished user experience	Poor application scalability, lack of request validation	Application scaling, input validation	Medium
Elevation of Privilege	Unauthorized escalation of user privileges	CAPEC-195	Unauthorized data access, control over systems	Weak access controls, insufficient user role separation	Principle of least privilege, regular access reviews	High
	Unauthorized administrative access	CAPEC-2	System compromise, unauthorized changes	Weak admin credentials, lack of admin role separation	Strong admin authentication, admin role separation	Medium
	User account manipulation	CAPEC-5	Unauthorized actions, data loss	Insufficient user role verification, lack of access control checks	Role-based access control, access control checks	Medium

STRIDE THREAT MODEL (RISK Mitigation)				
Threat Category	**Threat Description**	**Priority**	**Recommended Actions**	**Action Needed**
Spoofing	Unauthorized access	High	1. Implement strong authentication mechanisms. 2. Enforce multi-factor authentication.	Transfer
	User impersonation	Medium	1. Deploy robust user verification processes. 2. Continuously monitor user activity for anomalies.	Treat
	Digital identity forgery	Medium	1. Strengthen authorization protocols. 2. Implement identity verification for critical actions.	Transfer
Tampering	Data modification	High	1. Implement strong data validation mechanisms. 2. Use cryptographic signatures to verify data integrity.	Treat
	Product info alteration	Medium	1. Implement strict data validation for product information. 2. Strengthen access controls over product data.	Treat
	Order details change	Medium	1. Use secure channels for data transmission. 2. Implement robust order validation mechanisms.	Treat
Repudiation	Action denial	High	1. Implement comprehensive transaction logging. 2. Use digital signatures to ensure non-repudiation.	Treat
	False order denial	Medium	1. Implement thorough order tracking and logging. 2. Use digital evidence to prove order authenticity.	Treat
	Transaction repudiation	Medium	1. Strengthen transaction verification processes. 2. Implement non-repudiation mechanisms for transactions.	Treat
Information Disclosure	Unauthorized access	High	1. Enhance access control mechanisms. 2. Implement strong encryption for sensitive data.	Transfer
	Customer data exposure	Medium	1. Implement secure storage solutions. 2. Encrypt sensitive customer data at rest.	Treat
	Strategy leak	Medium	1. Implement strong access controls for strategic documents. 2. Require non-disclosure agreements (NDAs) for sensitive information.	Treat
Denial of Service	Service disruption	High	1. Implement DDoS protection measures. 2. Set up redundant systems to handle traffic spikes.	Treat
	Network congestion	Medium	1. Implement network monitoring solutions. 2. Analyze traffic patterns for anomalies.	Treat
	Application floods	Medium	1. Enhance application scalability. 2. Implement input validation to prevent flooding attacks.	Treat
Elevation of Privilege	Unauthorized escalation	High	1. Strengthen access controls and permissions. 2. Implement proper user role separation.	Treat
	Unauthorized admin access	Medium	1. Implement strong admin authentication mechanisms. 2. Enforce strict separation of admin roles.	Treat
	User account manipulation	Medium	1. Implement robust role-based access controls. 2. Regularly review and update user access rights.	Treat

5. Summery & Recommendations

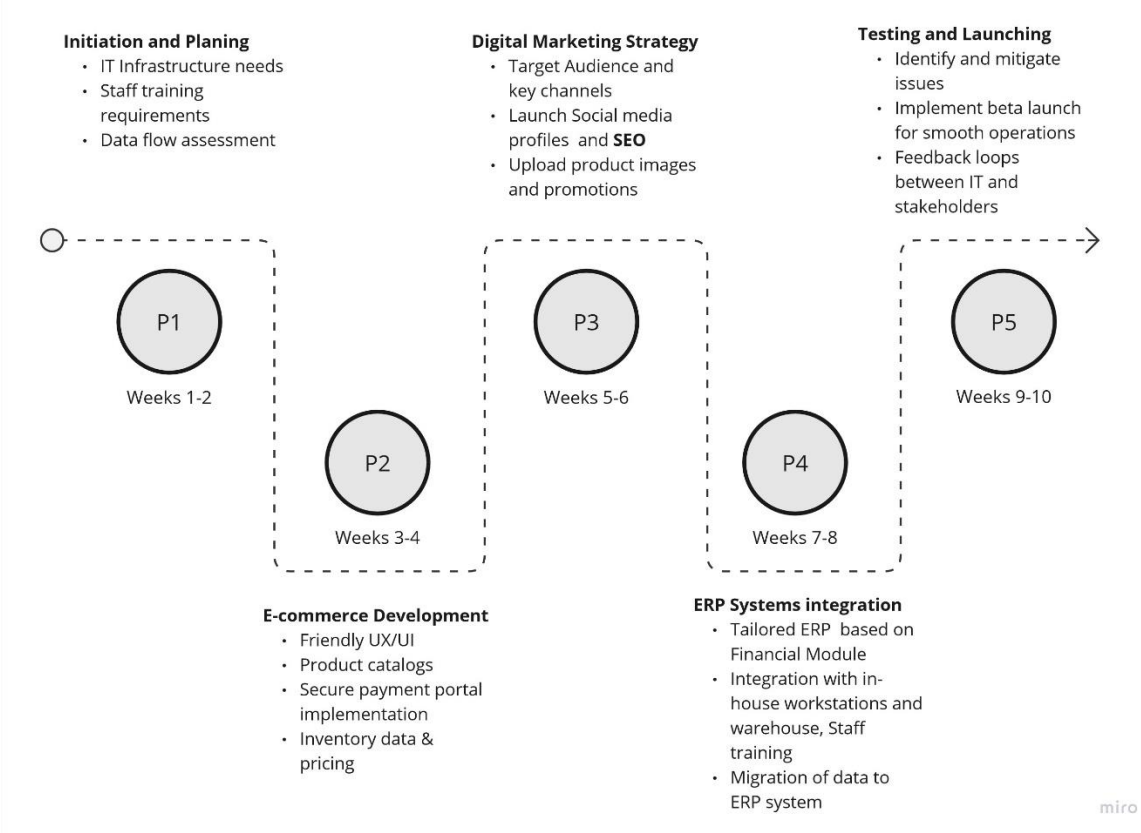
Given the numerous benefits offered by the digitization of this business model, along with the consideration of the identified associated risks, **it is strongly recommended the Pampered pets undergo the transformation process.**

Based on the risk assessments on the digitized model, an increased risk factor is evident. Consequently, risk mitigation strategies must be carefully considered by encompassing robust security measures, data protection protocols, and consistent vulnerability assessments. Furthermore, Pampered Pets must have the ability to address other challenges such as privacy compliance, system integration and financial risks.

Nonetheless, the adoption of this digitization process holds a potential increase in customer reach, enhanced supply chain, and informed decision making.

Digitization Timeline:

Finally, the following diagram suggests a 5 – step timeline of 10 weeks that is required for Pampered Pets to undergo a digitization process of their current business model:



References

Khan, R., McLaughlin, K. & Laverty, D., 2017. *STRIDE-based threat modeling for cyber-physical systems.* Turin, nnovative Smart Grid Technologies Conference Europe .

Lalonde, C. & Boiral, O., 2012. Managing risks through ISO 31000: A critical analysis. *Risk Managment ,* 14(3), p. 272–300 .

Mircosoft, 2009. *The STRIDE Threat Model.* [Online]
Available at: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN
[Accessed 23 08 2023].

Yuan, X., Nuakoh, E. B. & Yu, H., 2014. *Retrieving relevant CAPEC attack patterns for secure software development.* New York, Association for Computing Machinery.