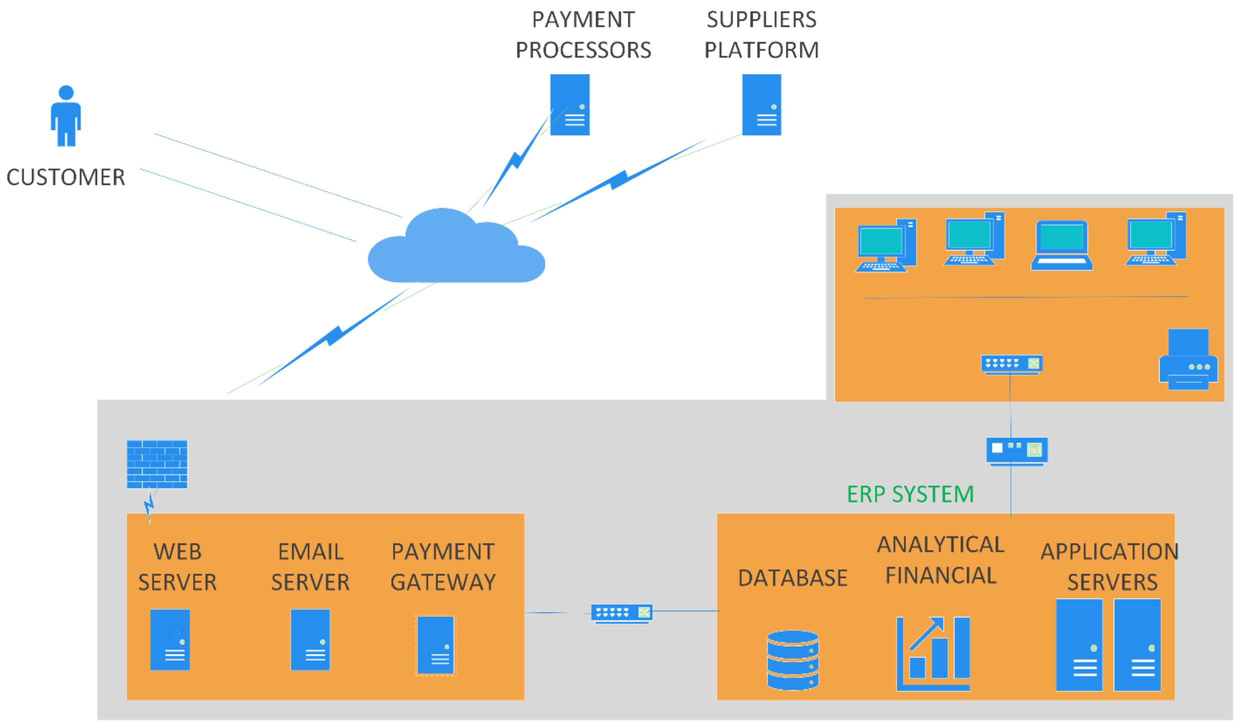
Case 2: **risk assessment after** digitalization

a. The proposed Digital transformation for Pampered Pets business

The following diagram shows the proposed change in order to perform the required digital transformation.

PAMPERED PETS
DIGITAL TRANSFORMATION DIAGRAM



The digitalisation process of Pampered Pets business wiil include

- Fully functional and response website that provide items description, prices, account creation for customers, ordering, order tracking
- Online payment functionality that accept most of payement card and payball
- ERP system that include HR, financial applications, stock management, sales
- Applications to orders items from suppliers
- Local networks seperated from the two other networks where employees can perform their daily tasks and connect to other functionality

b. Risk assessment methodology

In this report we will be using qualitative risl assessment Methodology since we don’t have the value of assets, associated risk and loss for each assets in dollar values. As such we can use risk matrix in which we categorize risks on rough scales such as High, Medium, or Low.

Risk Assessment Approach

This initial risk assessment was conducted using the guidelines outlined in the *NIST SP 800-30, Guide for Conducting Risk Assessments*[1]. A *QUALITATIVE* approach will be utilized for this assessment. Risk will be determined based on a threat event, the likelihood of that threat event occurring, known system vulnerabilities, mitigating factors, and consequences/impact to mission.

[1] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

c. Risk assessment

1. Identification of threats

Threat		Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
Natural Threats						
1	Fire/Smoke in Pampered Pets daya center.	An accidental or intentional fire could damage system equipment or facility.	√	√		
2	Acts of Nature	Hurricanes, tornadoes, flood according to the location of Pampered Pets business	√	√		√
Human Threats						
3	Espionage/Sabotage	Espionage is the intentional act of or attempt to obtain confidential information stored in Pampered Pets data storage. Sabotage is premeditated destruction or malicious modification of Pampered Pets' assets or data.	√	√	√	√
4	Theft/Pilferage	Theft is the unauthorized removal of computer equipment or media. Pilferage is theft of property by personnel granted physical access to the property.	√			√

Threat		Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
5	Hacking/Social Engineering	Software may be modified intentionally to bypass system security controls, manipulate data, or cause denial of service. Social engineering is the human-to-human interaction in which a hacker gathers data for use in modifying or manipulating the system.	√		√	√
6	Malicious Code	Malicious software such as viruses or worms may be introduced to Pampered Pets' system, causing damage to the data or software.	√	√	√	√
7	User Errors/Omissions	Pampered Pets's application and support system components may be inappropriately modified or destroyed due to unintentional administrator or user error.	√	√	√	√
8	Eavesdropping/interception	Intentional unauthorized access to confidential information through technical means (sniffing/interception) or by personnel having some level of system access but not having a need to know (eavesdropping)				√
9	Data Integrity Loss	Attacks on the integrity of Pampered Pets' system data by intentional alteration. For example changing the order / price / customer information in Pampered Pets systems.			√	

Threat		Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
10	Misuse/Abuse	Individuals may employ system resources for unauthorized purposes.	√	√	√	√
	Environmental and Physical Threats					
11	Power Disruption	A power failure or fluctuation may occur as the result of a commercial power failure inside Pampered Pets facility. This may cause denial of service to authorized users (failure) or a modification of data (fluctuation).	√		√	
12	Hardware/Equipment Failure	Failure or malfunction of hardware may cause denial of service to system users. Additionally, hardware configuration may be altered in an unauthorized manner, leading to inadequate configuration control or other situations that may impact the system.	√		√	√
13	Program Errors/Software Failure	Software malfunction or failure resulting from insufficient configuration controls (i.e., testing new releases, performing virus scans).	√	√	√	√
14	Communication Loss	Communication links may fail during use or may not provide appropriate safeguards for data.	√		√	√

2. Risk evaluation

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

Table 2: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the threat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event

Table 3: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times per year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Table 4: Assessment Scale – Impact of Threat Events

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Qualitative Values	Semi-Quantitative Values		Description
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Table 5: Assessment Scale – Level of Risk

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Qualitative Values	Semi-Quantitative Values		Description
High	80-95	8	Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 6: Assessment Scale – Level of Risk (Combination of Likelihood and Impact)

Likelihood (That Occurrence Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

3. Risk Assessment Results

Threat Event		Likelihood (Tbl 2 or 3)	Impact (Table 4)	Risk (Tbls 5 & 6)
1	Fire/Smoke in Pampered Pets daya center.	*Moderate*	*High*	*Moderate*
2	Acts of Nature	*Moderate*	*Moderate*	*Moderate*
3	Espionage/Sabotage	*High*	*Moderate*	*Moderate*
4	Theft/Pilferage	*High*	*Moderate*	*Moderate*
5	Hacking/Social Engineering	*Moderate*	*Moderate*	*Moderate*
6	Malicious Code	*High*	*High*	*High*
7	User Errors/Omissions	*High*	*Moderate*	*Moderate*
8	Eavesdropping/interception	*Low*	*Moderate*	*Low*
9	Data Integrity Loss	*Moderate*	*High*	*Moderate*
10	Misuse/Abuse	*Moderate*	*Low*	*Low*
11	Power Disruption	*Moderate*	*Moderate*	*Moderate*
12	Hardware/Equipment Failure	*High*	*High*	*High*
13	Program Errors/Software Failure	*Moderate*	*High*	*moderate*
14	Communication Loss	*moderate*	*High*	*moderate*

3. Potential mitigations

Threat Event		Mitigation
1	Fire/Smoke in Pampered Pets daya center.	*Install and Maintain Fire Control and Suppression Systems* - **Install a sprinkler, foam system, or other fire control and suppression system** - **Install fire alarms and smoke detectors** - **Establish and promote a fire safety plan and an evacuation plan**
2	Acts of Nature	**Mitigate hurricane: boarding up windows and doors, placing sandbags outside building openings, and installing a backup power system to keep all critical assets working**. Mitigate flood: use **floodplain protection** **The second option will be to buy inssurance**
3	Espionage/Sabotage	*Implement encryption system*
4	Theft/Pilferage	*Implement strict access control system* *Use system auditing and log* *Physical access control system*
5	Hacking/Social Engineering	*Install firewall / IPS / IDS* *Employee training and awerness*
6	Malicious Code	*Install antivuris and antimalware*
7	User Errors/Omissions	*Implement data verification and validation system* *Use auditing and journals* *User education and training*
8	Eavesdropping/interception	*Encryption* Using packet filtering configure routers and firewalls to reject any packets
9	Data Integrity Loss	*Implement Data loss prevention (DLP)* *Buy Software as a servuce (SAAS) cloud*
10	Misuse/Abuse	*Implement Need to know access*
11	Power Disruption	*Install* uninterruptible *power* supply (UPS)
12	Hardware/Equipment Failure	*Use redundent /failover hardware/ equipement* *Buy IAAS (infrastructure as a service) cloud (depending on the ROI that need to be evaluated if more dollar values is been provide)*
13	Program Errors/Software Failure	*Use program and software redundancy and backups* *Buy Software as a servuce (SAAS) cloud*
14	Communication Loss	*Use of redundent communication links* *Buy IAAS (infrastructure as a service) cloud*