MODULE-3

SECURITY & RISK MANAGEMENT

RISK ASSESSMENT | Group-3 | 16 SEPT 2022

PAMPERED PETS

RISK IDENTIFICATION REPORT

INTRODUCTION

To identify the risks and benefits under different scenarios, a risk assessment of the company Pampered Pets was performed.

Pampered Pets is currently looking to digitize their operation, and change from a local-area focused business, into a more global company. These transformations could bring big benefits to the business, but also carry significant risks.

Two risk analyses were performed, firstly on the current local business model, and secondly, on the proposed model of a larger, internationally operating business.

The method of Threat Modeling used for both assessments was the Quantitative Threat Modeling Method – QTMM (QTMM, 2022). QTMM allows us to combine different methodologies, to determine the perceived threat for each category, but also by using quantitative assessment, allows us to categorize the threats using more factual data (trustnetinc, ND).

Initially, an Attack Tree (**Threat Tree for Online Business**) was created (Isograph, ND), which allowed us to identify and classify some of the threats. The tree used Boolean OR logic, meaning, that any threat can be “standalone” OR credible, in conjunction with

other threat/s. We subsequently used a combination of STRIDE (STRIDE, 2021) and CVSS (CVSS, 2022) modeling, to rate and rank the different threats based on the quantitative scoring.

RISK ASSESSMENT 1 – BRICKS ‘N MORTAR (METHODOLOGY)

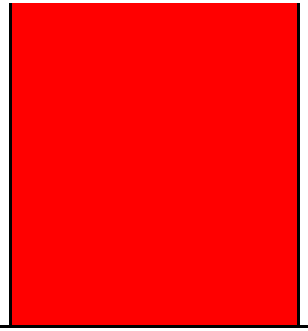
The following risk assessment assesses the existing business model.

Risk Register and Mitigation Plan

Risk No	Risk Details	Impact 1 - 5	Probability 1 - 5	Inherent Risk Rating (CALCULATION)	Mitigation Plan	Action Owner
Business Risks						
1	No Subscription to regulatory and compliance standards	5	3	15	Adoption of regulatory frameworks such as GDPR and PCI-DSS to ensure compliance	Alice
2	Supply Chain Risks - Inability for suppliers to	4	2	8	Incorporate a business continuity plan	Alice/Cathy

	deliver goods					
3	Scalability - Inability to handle increased sales	3	4	12	Increase human resource capacity and initiate a business process improvement initiative	Alice/Cathy
IT Risks						
4	Lack of IT security controls - emails susceptible to spoofing, spam, phishing. Usage of a spreadsheet more susceptible to data	5	5	25	Acquisition of ERP and ecommerce website hosted in the cloud to streamline operations centrally	Harry

	integrity errors, no data encryption.					
5	Legacy IT Security infrastructure - No security controls for Wireless connectivity, usage of a hub instead of switch, easier to compromise systems etc.	5	5	25	Implement a cyber security infrastructure program to provide comprehensive security for Wireless Network and Perimeter security, E-mail security, Cloud environment, endpoint security, and end-to-end encryption	Harry/Cathy
6	No Business Continuity Plan / Disaster recovery - Information resides on	5	3	15	Develop BCP/DR Plan	Andrea/Harry

	one computer and risk of losing data from hardware failure or theft is high.					

RISK ASSESSMENT 2 – DIGITALISATION

The following risk assessment assesses the proposed model after digital transformation.

Proposed changes to digital transformation

1. Deployment of a Cloud-based ERP Solution.

2. Develop and integrate an e-commerce website (Online Portal).

3. Cyber Security Managed Infrastructure which incorporates Cloud, e-mail, wireless, endpoint, perimeter and network security.

4. Compliance with legal and regulatory requirements globally to protect customer information and online transactions – GDPR and PCI-DSS and other relevant legal requirements.

5. An Information security program containing policies, processes, procedures to protect the business information assets.

1. **Risk Register and Mitigation Plan (METHODOLOGY)**

Risk No	Risk Details	Impact 1 - 5	Probability 1 - 5	Inherent Risk Rating (CALCULATION)	Mitigation Plan	Action Owner
Business Risks						
1	Local or International Legislation and regulatory requirements e.g., GDPR	3	3	6	Research international regulatory requirements and adoption	Alice
2	Supply chain risk - Local vs. International Business. Loss of local business and quality of products	4	5	20	Manage supply to meet demand to global community without compromising quality. Increase resources and	Cathy/Harry

					shopping capabilities globally. Develop global partnerships.	
3	New income forecasts are inaccurate.	2	2	4	During the initial discovery phase of the program, the management team should conduct focused due diligence before proceeding to the next phase.	Alice
4	Cultural Diversity - Language Barriers, Ethical considerations,	2	2	4	Partnership with international stakeholders to breach cultural barriers	Alice
5	Costs to expand globally – known and unexpected costs	3	3	9	Development of a financial plan and budget forecasting to meet costs	Alice/Cathy

6	Number of Staff Inadequate	2	4	8	Development of a human resource plan and provision of staff training	Cathy/Harry
7	Benefit/risk of digitization itself – loss of “community” feeling, lack of staff training etc. vs reaching wider customer audience and higher turnover	4	3	12	● Develop a training policy for current staff ● Develop an incentive program to encourage staff for self-education	All
8	Natural Disasters	5	1	5	Develop business continuity plan and disaster recovery plan	Alice
IT Risks						

9	Cyber Security attacks, cyber-crime, Data leakage	5	5	25	Implement a cyber security strategy and controls to protect against data leakage of personal information, hacking, malicious attacks on systems and infrastructure, and information security policies	Alice
10	IT skills capacity	2	4	8	Appointing adequate resources with the skills, and retraining staff	Alice/Cathy
11	Physical assets capabilities and availability	3	3	9	Replace legacy systems, build a redundant infrastructure and insure physical assets	Alice /Cathy

12	Inefficient IT service providers/Vendors/Partners	4	2	8	Transfer risk to service providers and agree on SLAs.	Alice/Cathy
13	Disaster recovery and business continuity	5	3	15	Creation of regular backups, and a cloud infrastructure with a disaster recovery site to allow business continuity	Andrea / Harry

RECOMMENDATIONS

The online presence could grow the business. It may increase brand awareness nationally or internationally, instead of only the local community — more people become aware of the brand. After, the business opportunities or brand franchise opportunities could grow the business 50%.

Changing to an International supply chain, incurs extra costs to partner with the warehouse and courier services provider. The way to reduce the cost, is to increase the visibility of inventory and delivery trace at any given time. These could chart the demands and the delivery issue, by introducing an inventory and delivery management system. It can reduce the unnecessary warehouse cost and re-delivery cost.

Alternatively, the traditional business model in the local area is still in place for the current customer. It is unlikely to lose existing customers even without some online features.

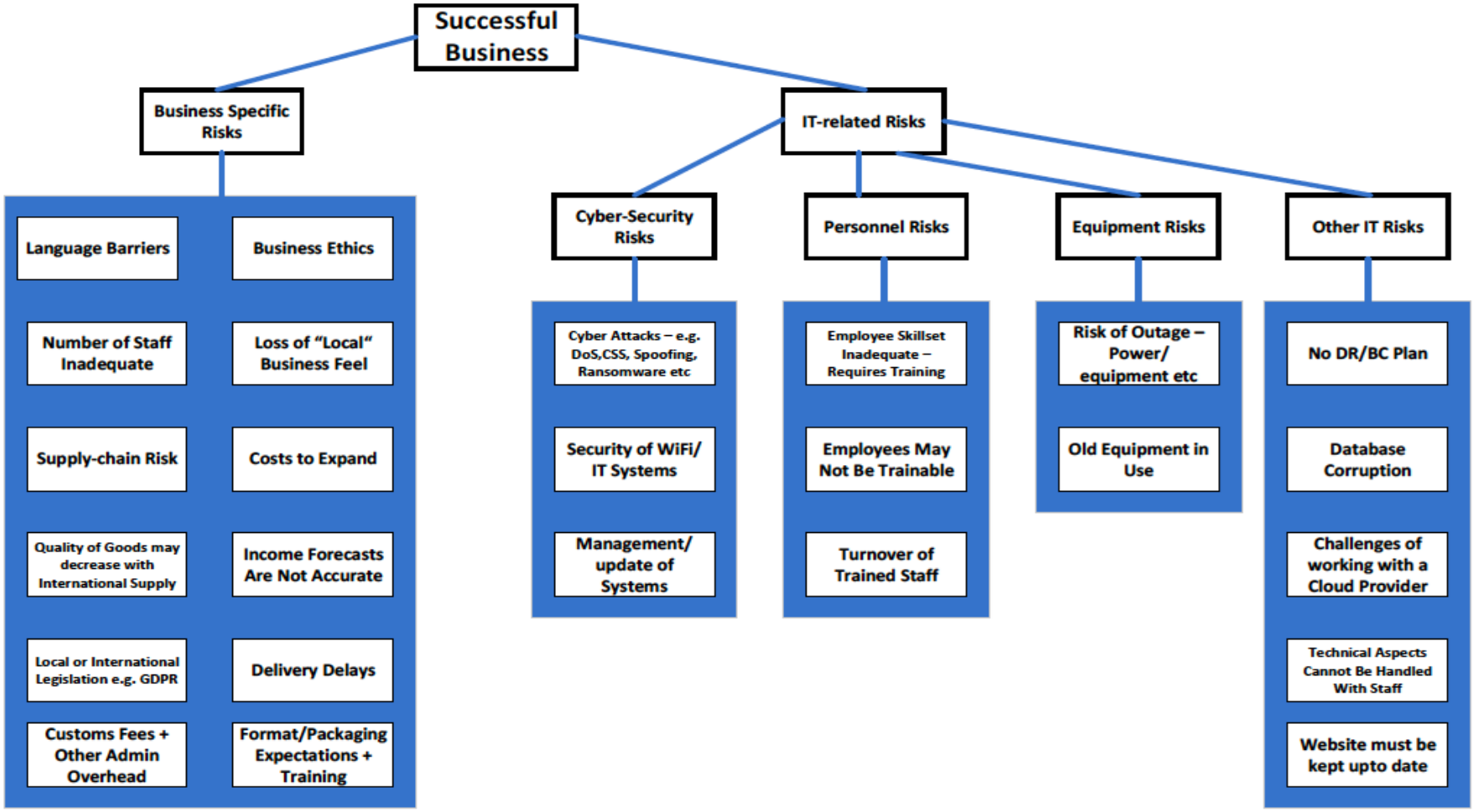
In conclusion, the digitisation process is recommended because of the increased brand awareness and business growth opportunities.

REFERENCES

1. QTMM, (2022). *What is Threat Modelling? 10 Threat Identity Methods Explained.* Available at: https://www.upguard.com/blog/what-is-threat-modelling [Accessed on 11 September 2022]
2. Trustnetinc, (ND). *Qualitative vs. Quantitative Risk Assessments in Cybersecurity.* Available at: https://www.trustnetinc.com/qualitative-vs-quantitative/ [Accessed on 11 September 2022]
3. Isograph, (ND). *Attack Tree Modelling in Attack Tree.* Available at: https://www.isograph.com/software/attacktree/creating-an-attack-tree/ [Accessed on 11 September 2022]
4. STRIDE, (2021). *STRIDE Threat Modelling: What You Need to Know.* Available at: https://www.softwaresecured.com/stride-threat-modeling/ [Accessed on 11 September 2022]
5. CVSS, (2022). *What is a CVE? Common Vulnerabilities and Exposures Explained.* Available at: https://www.upguard.com/blog/cve. [Accessed on 11 September 2022]
6. Thompson. R. (2019) *Overcoming the challenges and threats to effective digital transformation.* Available at: https://iiot-world.com/industrial-iot/connected-industry/overcoming-the-challenges-and-threats-to-effective-digital-transformation/ (Accessed on 22 August 2022).

APPENDICES

Threat Tree for Online Business -



This Threat Tree is based on BOOLEAN OR. Any of the threats within the boxes may apply singularly or in conjunction with other threats

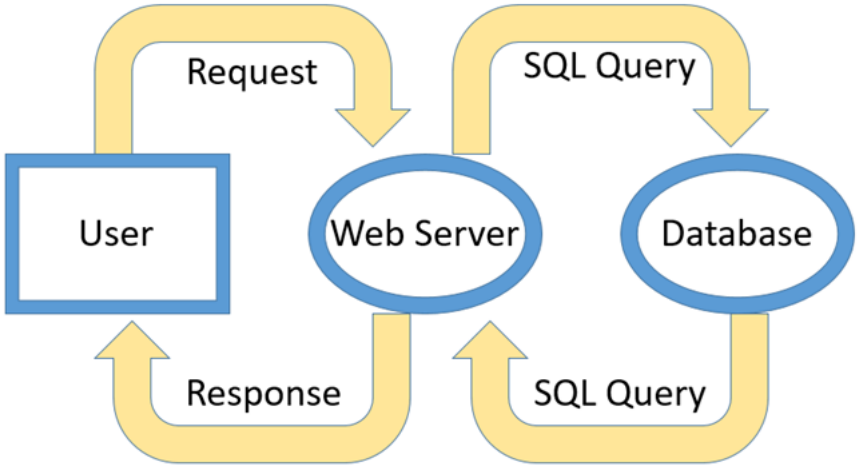


Figure 1 – System Data Flow

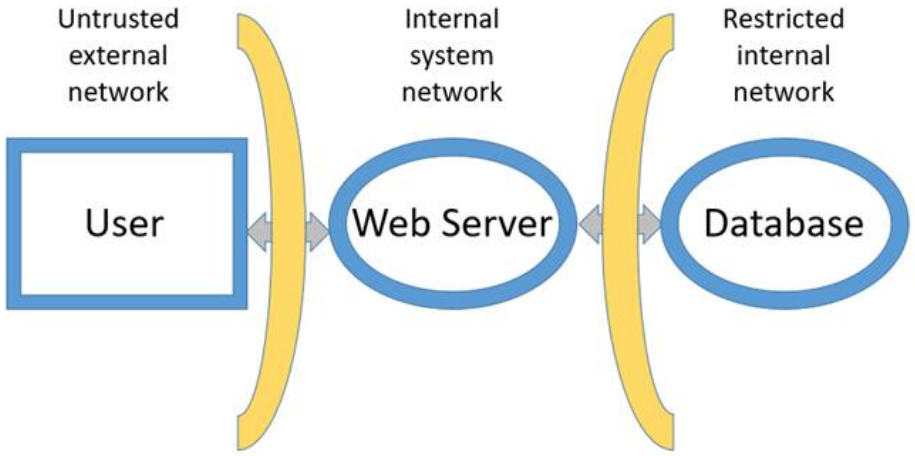


Figure 2 – System Attack Surface

STRIDE is one of the common threat modeling methods used to identify the threats to the system. Table 1 below shows the victims of the violation of the STRIDE threat model.

	Threat	Victims	Property
S	Spoofing	Processes, People	Can an attacker pretend to be a different user?
T	Tampering	Processes, Datastores, Data flow,	Can an attacker modify data used by the system?
R	Repudiation	Processes	Can an attacker deny that they acted to change the system state?
I	Information Disclosure	Processes, Datastores, Data flow,	Can an attacker extract sensitive information?

D	**Denial of Service**	**Processes, Datastores, Data flow,**	**Can an attacker exhaust system resources and make the system not function?**
E	**Elevation of Privilege**	**Processes**	**Can an attacker promote their privilege without an authorization?**

Table 1 – Victims of violations of the STRIDE Threat Modeling

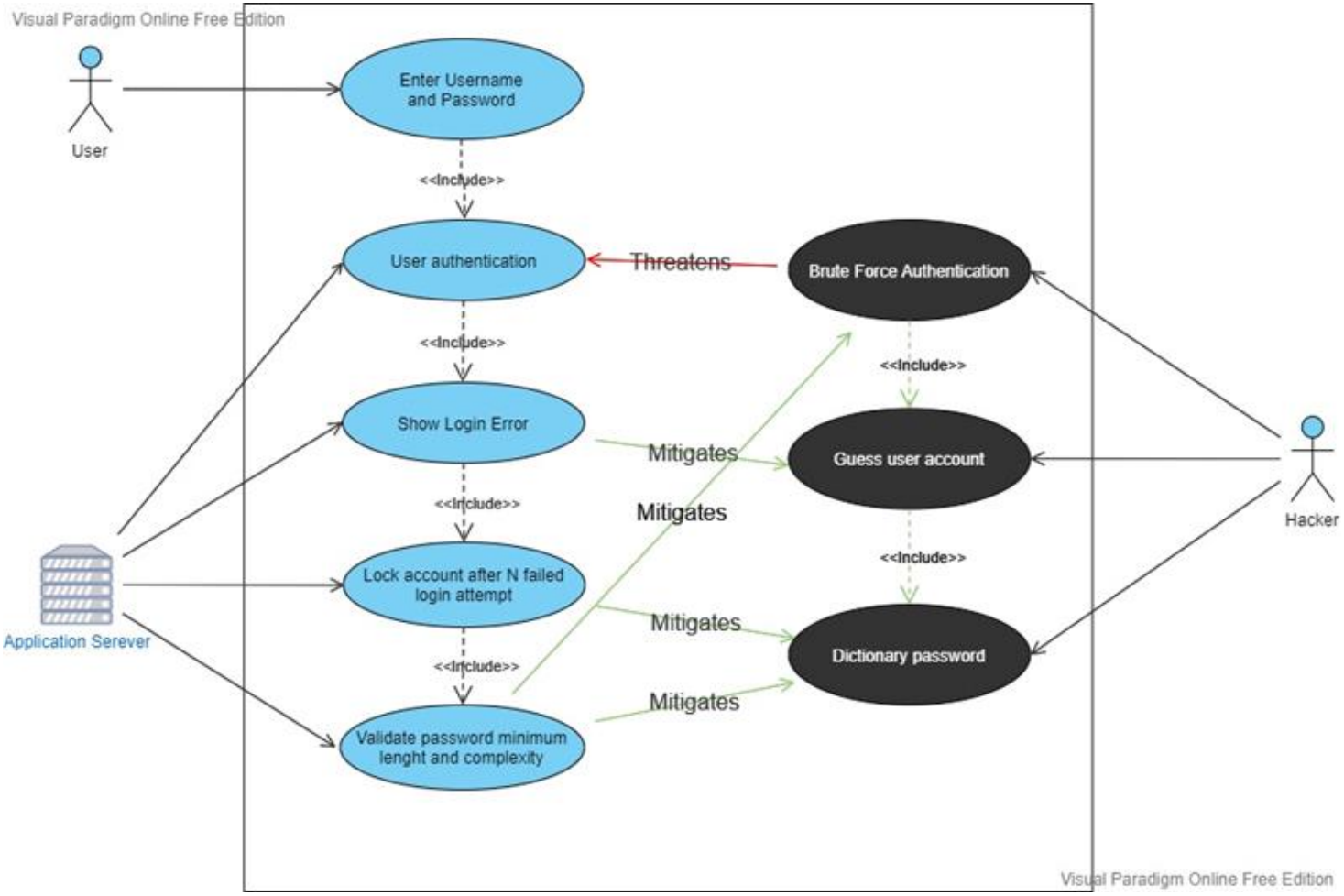


Figure 3 – Mitigation based on the STRIDE threat model

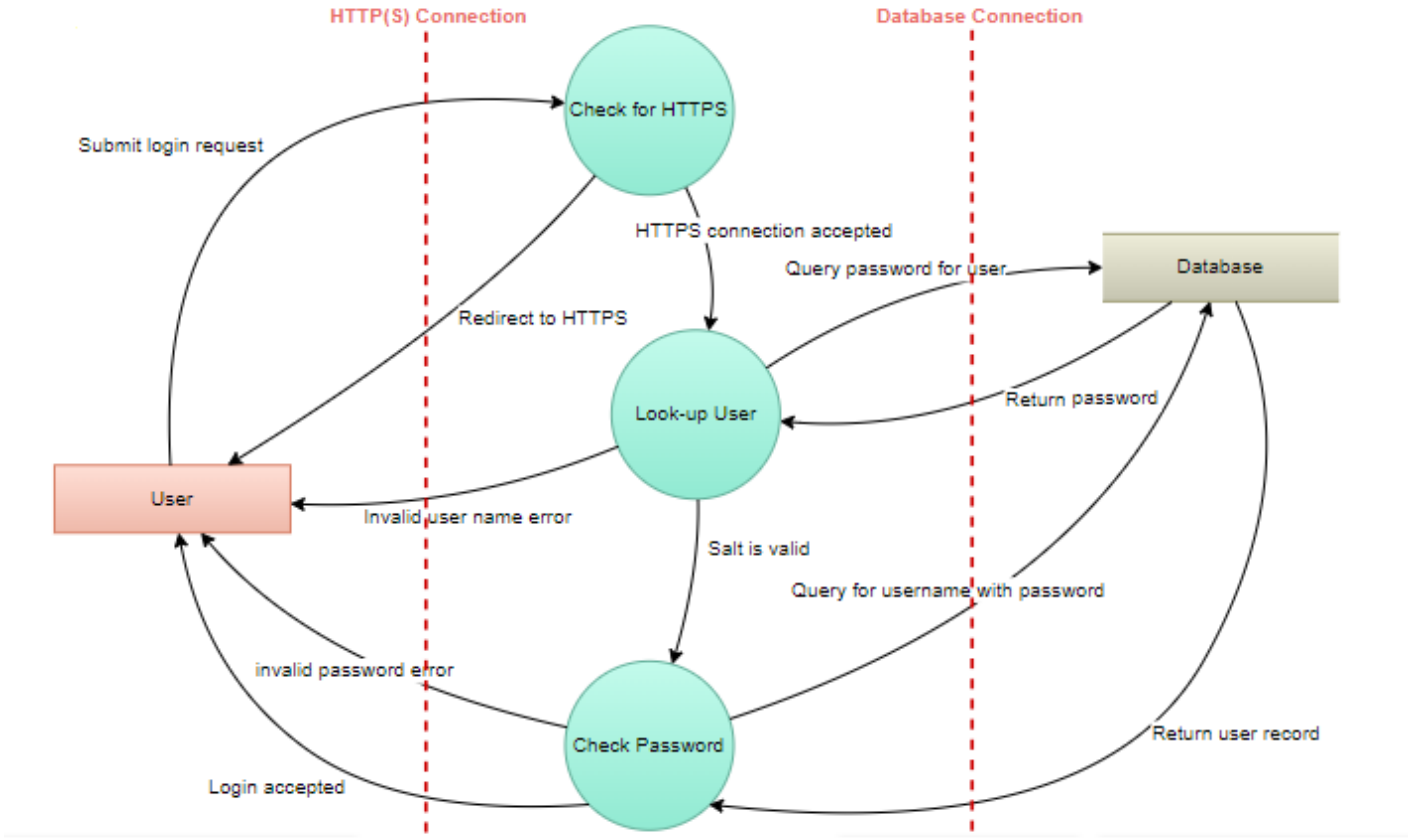


Figure 4 – Authentication Data Flow

METHODOLOGY FOR CALCULATING RISK

RISK RATING ELEMENTS - IMPACT

Risk	Critical	Major	Sizeable	Moderate	Minor
Level	5	4	3	2	1

RISK RATING ELEMENTS - PROBABILITY

Probability Of Occurrence	Under 10%	25%	50%	75%	Over 90%
Rating	1	2	3	4	5

RISK CALCULATION

Overall Risk Rating = Impact x Probability

RISK RATING CATEGORIES

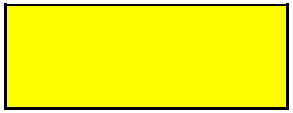
High Risks (Rating of 15-25)

These risks require immediate attention and, as a high priority, a plan needs to be put together to provide sufficient mitigation resulting in a lower rating for the residual risk, wherever possible.

Medium Risks (Rating of 6-12)

Controls should be put in place to mitigate the risk, wherever possible, especially where the risk is close to the risk tolerance level, or is increasing over time.

Low Risks (Rating of 1-5)



No action required to mitigate these risks.

Overall Risk Rating Matrix

		Probability				
		1	2	3	4	5
Impact	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25