CSG3309 Case Study Confidential Report-John-DOUGH.

Assessment 2

Project Proposal
For JOHN DOUGH

Prepared by:

Lovya Bajaj: 10565489

Manoj Bhandari: 10583441

Ishita Chopra: 10599428

Campus: Joondalup Campus

Department of Science

Submitted to:

Leah Shanley

Table of Contents

EXECUTIVE SUMMARY

The following is the Project Proposal as requested by your side which shows how information security of JOHN DOUGH can be protected. We have used several tables and a flowchart to help you understand the project description our company will be implementing. JOHN DOUGH still looks like it is on its earliest stages of development and therefore, it lacks a lot of security measures. Please analyse the document and let us know when you want us to start with the project.

INTRODUCTION

This paper holds a strategy for asset identification and prioritisation, as well as a risk assessment, for John Dough, a pizza delivery and dine-in restaurant. The plan describes the asset types, who owns them, and the criteria used to prioritise them. The influence on income, R&D, secrecy, availability, integrity, and public image are among the factors. The identification of assets, possible threats, vulnerabilities, likelihood, impact, and total risk is part of the risk assessment. Because of ambiguous information, several assumptions were made. The plan's goal is to help John Dough in understanding his company's essential assets and how our company will help him protect them as well as achieve his 5-year business goals.

ASSUMPTION

Following are some of the assumptions we made to complete our tasks since some of the information supplied was unclear:

For Asset Identification:

Asset Owner of employees, legal managers, accounting and finance division, R&D division, Board Members, and employees in asset identification should be HR Head but since no word of HR is given, we have used CEO instead.

Similarly, since no word or Network Analyst is given, we have used IT Team as the asset owner for Network equipment, servers etc.

SCOPE

The document is to provide John Dough with the plan of the project which is in best favour of the information security of the company. The project plans follow the laws and regulations and includes several risk control measures which are perfect for JOHN DOUGH.

It covers the scope of work for John Dough, a pizza restaurant business, in terms of asset identification, prioritisation, and risk assessment. Following a thorough asset table categorising assets into hardware, software, infrastructure, people, and information, the paper includes a summary of the assumptions made during the process due to imprecise information presented. The chart also includes the asset owners for each category and ranks assets according to their influence on R&D, secrecy, availability, integrity, income, and public image. The paper also discusses why these characteristics were utilised to decide asset priority.

Furthermore, the document assesses each asset's risk by finding the danger, vulnerability, likelihood, impact, and risk rating. The risk assessment supports in the formulation of a risk management strategy by helping to understand the possible hazards connected with each asset.

Based on the information supplied, the scope of this paper is restricted to asset identification, prioritisation, and risk assessment for John Dough. The paper does not hold asset management risk reduction measures, risk management plans, or any legal or regulatory requirements. The paper is meant to offer a detailed analysis of the assets and associated risks to aid John Dough in making educated asset management and risk reduction choices.

ASSET IDENTIFICATION AND PROORITIZATION

Looking at the JOHN DOUGH confidential report, our team have listed the important assets of the company below along with their owners and the category they belong to. Finding the risks will help us work on prioritising them and then find the controls for the associated with these assets.

Asset Category	Asset Element	Asset Owner
Hardware	Computers (e.g., Mobile phones for ordering food)	Users
	Computers (e.g., Desktops, laptops)	CTO
	Computers peripherical (e.g., printers)	CTO
	Network equipment (e.g., network cabling, firewalls, switches, routers, hubs, Bluetooth, and VoIP devices, Wi-Fi connections, servers)	CTO
	Preparation equipment (benches, Food tray, Pizza proofing trays, Oven pans, Mixing equipment, pizza ovens)	Corporate Officer
	Dine-in equipment (e.g., tables, chairs, ordering counter)	Corporate Officer
Software	Sales System	R&D
	Stocker2000 V1.0.0	CTO
	JOHN DOUGH online software	CTO
	JOHN DOUGH Q-Message	CTO
	Xero Software	Accounting and Finance
	Application Software (Word, Office suits, e-mails)	R&D
Information (in physical or electronic form)	Employee Database (e.g., salary, addresses, contact numbers etc.) and Customer Database (e.g., order history, contact numbers, addresses, card information etc.)	R&D
	Contract documents (e.g., contracts with customers, franchises, and suppliers)	Franchise Operator
	Websites and social media accounts	CTO

	Financial Documents (e.g., expense, income, transaction history, invoices etc.)	Accounting
	Manuals (for training purposes)	R&D
	Internal Documents (plans, reports, password files)	R&D
	Legal Documents (e.g., Loan documents)	Corporate Officer
	Franchise Operations and Sales Records	Franchise Operations Provider
	Communication records (e.g., customer emails, business emails etc.)	CTO
Infrastructure	Installations (warehouses, buildings, offices)	Corporate Officer
People	Legal managers	CEO
	Accounting and Finance division	CEO
	R&D Division	CEO
	Employees	CEO
	Customers	User

Table 1.1: Assets Identification. Used Asset List for ISO-27001.

Table given below stands for the WFA (Weighted Factor Analysis)

Asset Category	Information Asset	Criterion 1: Impact on R&D	Criterion 2: Impact on Confidentiality, Availability, and Integrity	Criterion 3: Impact on Revenue	Criterion 4: Impact on Public Image	Weighted score
Criteria Weights = 100		30	30	20	20	
Hardware	Network Equipment	0.4	0.8	0.2	0.2	44
Software	Sales System	0.5	0.3	0.1	0.1	2
	Stocker2000 V1.0.0	0.4	0.2	0.2	0.1	24
	JOHN DOUGH online software	0.3	0.8	0.9	0.8	67
	JOHN DOUGH Q-Message	0.5	0.8	0.5	0.8	65

	Xero Software	0.3	0.5	0.3	0.1	32
Information (in physical or electronic form)	Customer and employee Database	0.8	0.9	0.8	0.9	85
	Website and Social Media accounts	0.6	0.9	0.7	0.8	75
	Financial Documents	0.5	0.9	0.6	0.7	30
	Legal Documents	0.7	0.7	0.5	0.3	58
	Franchise Operations and Sales Records	0.7	0.8	0.6	0.6	69
Infrastructure	Installations	0.6	0.6	0.8	0.5	62
People	Employees	0.8	0.7	0.7	0.6	79
	Customers	0.6	0.7	0.9	0.8	73
	Accounting and Finance Division	0.7	0.6	0.7	0.4	61

Table 1.2: Weighted Factor Analysis (used NIST SP 800-14, NIST SP 800-100). (Wilson & Hash, 2003)

After prioritising the important assets, we discovered that customer and employee database should be at priority and mainly the customer database. Since, customers are vital for a business to grow, their information and their data should be secured with a company including all their bank details, phone numbers etc.

This will also make the company follow the Privacy Act and protect its reputation within the market.

Why are above factors used for calculating the priority for assets?

It is important to figure out the factors necessary for prioritizing the assets. We have used four assets which includes impact on R&D, impact on confidentiality, availability and integrity, impact on revenue and impact on public image.

Since, the five-year plan for JOHN DOUGH includes expanding the company and being at the top when it comes to preparing pizzas with the most innovative ideas, resource and Development should be considered an important asset. Impact on confidentiality, availability and integrity have been considered since these are the aspects which makes a company trustworthy. Furthermore, revenue and public image is used since these aspects will help JOHN DOUGH create profit and more franchises to partner with, respectively. Therefore, the above aspects have been chosen quite thoughtfully to help John Dough understands the vital assets of his company according to his plan.

RISK ASSESSMENT

Asset ID	Category	Asset	Threat	Vulnerability	Likelihood	Impact	Risk Rating
01	Hardware	Network Equipment	Technological Obsolescence	Lacks security updates and patches	Low	High	5
02	Software	Stocker2000 V1.0.0	Technical software failures or errors	Includes legacy code and risk of data failure	Low	High	6
03	Software	JOHN DOUGH online software	Software Attacks	Defecting the software with malicious code	Moderate	High	7
04	Information	Customer and employee Database	Espionage or trespass	Loss of confidential records to	High	High	8
05	Information	Franchise Operations and Sales Records	Espionage or trespass	Risk of losing confidential reports to wrong hands	Low	High	8
06	Infrastructure	Installations	Theft	Physical attacks and theft of important assets.	High	High	7
07	People	Employees	Information extortion	Disclosing confidential information	High	Moderate	6
08	People	Customers	Human error or failure	Reacting to phishing emails and losing important data	Moderate	Moderate	6

Table 2.1: Risk Assessment (used NIST 800-30, NIST 800-50). (Wilson & Hash, 2003)

RISK CONTROL

The following is the Risk Register and shows the main risks associated with the assets and what control would be needed to either defend, mitigate, accept or end them.

Risk ID	Description	Likelihood	Consequence / Impact	Level of Risk /Rating	Priority	Control	Description of Control
1.0	Power outage due to natural disaster or other circumstances	Low	Major	Moderate	High	Accept	Control: ISM-1511, Control: ISM-1515; The disaster recovery exercise, restoration of data, software and configuration settings are tested to a common point in time
2.0	Unauthorised access to network	High	Serious	High	High	Detect, Protect, Respond	Running automated vulnerability scans, applying patches where necessary and using risk rating to solve the vulnerabilities detected.
3.0	Employee errors	High	Major	Moderate	Moderate	Mitigate	Implementation of skills gap analysis, filling of gaps with training, implementing a security awareness program NIST SP 800-50 Infosec Awareness Training
4.0	Theft or damage of hardware equipment	low	Major	High	Moderate	Defend, Mitigate	Locks, ID cards could be used. CCTV cameras to be installed. Security guards must be kept.
5.0	Cyberattack threats	Moderate	Major	Very High	High	Defend, Accept	Control: ISM-1409; Making operating systems more secure with vendor and ACSC recommendations. Control: ISM-0576; A plan for responding to incidents is created,

							put into effect, and supported together with an incident management policy.
6.0	Online ordering system affected with malicious code	High	Major	High	High	Protect, Detect	Using anti-malware software, using anti-exploit technologies
7.0	Un-controlled Use of Administrative Privileges	Moderate	Major	Major	High	Protect	Cis Comtrol 4: Using dedicated workstations for all administrative tasks
8.0	Unauthorised access to facilities	Low	Major	High	High	Detect, Protect	Cis Control 4: Keeping Inventory of Administrative accounts, changing passwords, using multi-factor authentication
9.0	Access to unencrypted databases in wrong hands	High	Major	High	High	Protect	Control: ISM-0393 Protecting databases with end-to-end encryption and restricting employees from changing the databases according to their level.
10.0	Loss of data due to human error	Moderate	Serious	High	High	Protect	Keeping regular backups and then keeping the backup safe. Every backup should always have at least one offline destination.

Table 3.1: Risk Controls for risks shown (Used CIS Controls and ISM (Information Security Manual)).
(*Information Security Manual (ISM) | Cyber.gov.au*, 2023).

WORK BREAKDOWN STRUCTURE (WBS)

Work Breakdown structure gives the idea of how the tasks will be divided and how each part of the security project will be considered by our team with complete focus.

The table also shows he estimated time needed for each step along with the cost and budget needed.

Task No.	Task Description	Dependency	Resources Needed	Task Status	Cost	Start Date	Estimated Completion	Finish Date	Compliance
1	Initiate phase	n/a		Completed	$0	12/05/2023	13/05/2023	13/05/2023	EISB: Compliance planning- Follow all laws and regulations and are communicated to the proper channels
1.1	Perform assets identification	n/a	Team	assigned	$0	14/05/2023	16/05/2023	15/05/2023	Identification of applicable legislation and contractual requirements- ensuring compliance with relevant legislation and regulation of information security
1.2	Find project stakeholders	1.1	Risk assessment team (RA),	Not started	$100	16/05/2023	20/05/2023	20/05/2023	n/a
1.3	Define project goals and aims	n/a	Project manager (PM), team	Not started	$1500	21/05/2023	01/06/2023	01/06/2023	Compliance with the project statement and stakeholder requirements
1.4	Conduct initial risk assessment	1.1	PM team, RA team	In progress	$500	02/06/2023	06/06/2023	06/06/2023	Identification of applicable legislation and contractual requirements- ensuring compliance with relevant legislation and regulation about

									information security
2	Planning phase	1	PM team, team	In progress	$1000	07/06/2023	20/06/2023	20/06/2023	Compliance with security policies and standards
2.1	Develop and define project plan	n/a	PM team, team	In progress	$200	21/06/2023	30/06/2023	30/06/2023	Compliance with security policies and standards when it comes to developing and planning
2.2	Create schedule and find resource requirements	2.1	PM team, Security implementation team (SI)	Not started	$50[i]	01/07/2023	07/07/2023	07/07/2023	Develop and implement which include information security and controls
2.3	Name and evaluate risks	2.2	SI team, Security policy and compliance team (SPC)	Not started	$0	08/07/2023	10/07/2023	10/07/2023	Define and apply information security risk that include the risk acceptance criteria and criteria for performing information security risk assessment
2.4	Develop risk response plan, DRP and BCP	2.3	SI team and SPC team, PM team	Not started	$50	11/07/2023	13/07/2023	13/07/2023	When developing the risk response plan, it's in compliance with the contingency planning for example the disaster recovery, incident response and

									longevity of the business
3	Execution phase	2	PM team, SPC team	In progress	$3000	14/07/2023	24/07/2023	24/07/2023	Privacy Act is considered
3.1	Buy and install equipment and systems	n/a	PM team, RA team	Not started	$10000	24/07/2023	20/08/2023	20/08/2023	In compliance with equipment siting and protection, equipment maintenance, cabling security and supporting utilities
3.2	Develop the new online ordering system	3.1	PM team, developers	Not started	$10000	21/08/2023	05/09/2023	05/09/2023	In compliance with secure development policy, DRP, secure development environment and security testing
3.3	Upgrade stoker2000 system	3.1	Programmers, PM team, SPC team	Not started	$5000	06/09/2023	20/09/2023	20/09/2023	In compliance with development, testing and operational environments to reduce risk of unauthorised access to the stoker2000 system
4	Control phase	3	PM team, team	Not started	$0	21/09/2023	23/09/2023	23/09/2023	N/A
4.1	Monitor projects progress	2.1,3.2,3.3	PM team, team	Not started	$0	24/09/2023	27/09/2023	27/09/2023	In compliance with monitoring, incident response measurement, analysis and evaluation

4.2	Manage project changes	4.1	PM team, team, SPC team	Not started	$0	28/09/2023	30/09/2023	30/09/2023	The planned changes are controlled and have been reviewed for consequences and taking any action on any massive affects moving forward
5	Closing	4	PM team, team	Not started	$0	01/10/2023	03/10/2023	03/10/2023	N/A
5.1	Deliver the project	n/a	PM team, team	Not started	$0	04/10/2023	05/10/2023	05/10/2023	Deliver the project in compliance with information security policy and standards
5.2	Close the project	5.1	PM team, team	Not started	$0	06/10/2023	10/10/2023	10/10/2023	N/A

Table 4.1: Work-Breakdown structure.

Following is the flowchart showing the WBS (WORK BREAKDOWN STRUCTURE).

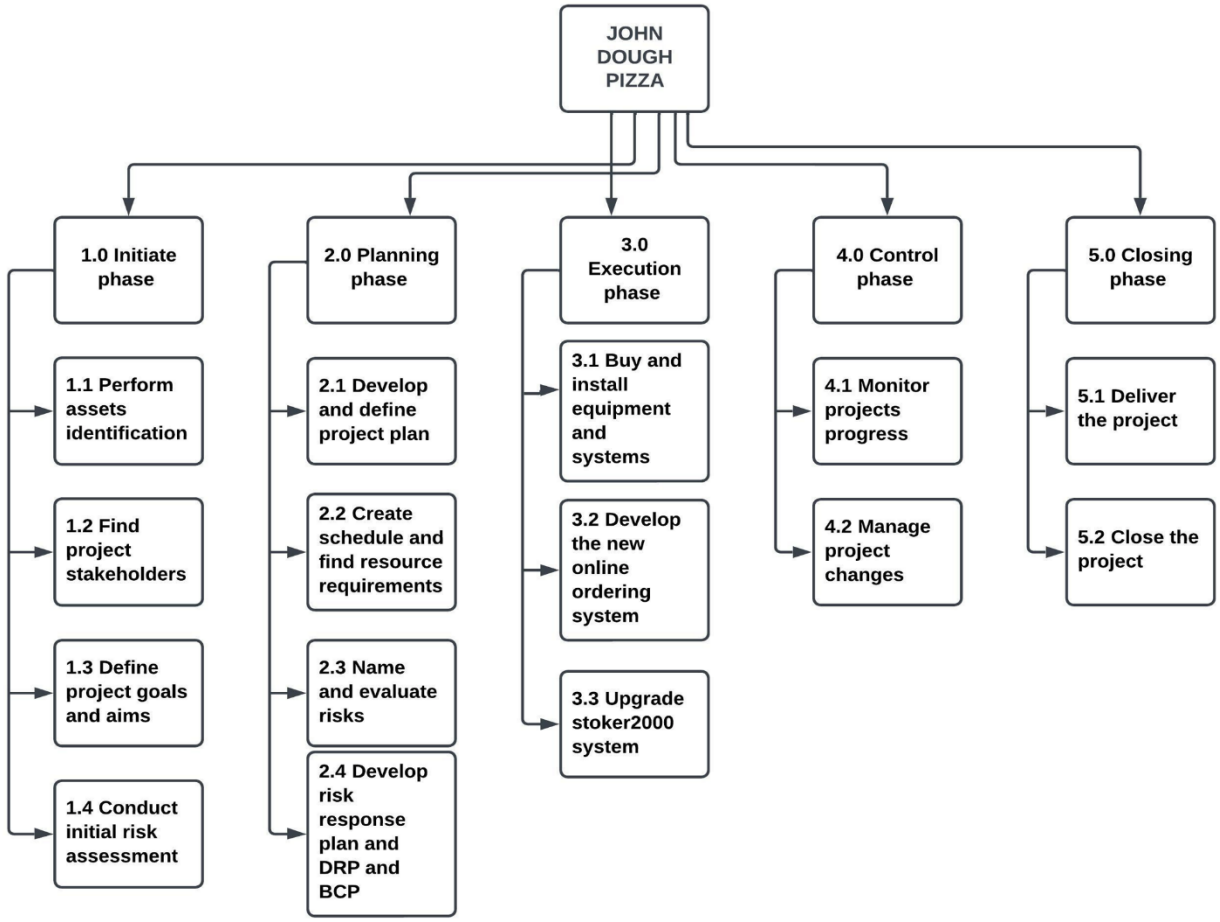

Chart 4.1: Work Breakdown Structure in a flowchart.

FUTURE PROGRAMS

When it comes to future security programs, research, and improvement we need to glance at the risk assessment conducted and 5-year goal plan of John Dough pizza. For these risks, the following future projects can be addressed.

Hardware security - Since John Dough uses a lot of technology to conduct their business having reliable security for this technology. John Dough needs to have encrypted level security on hardware and sensitive devices (Ashtari, 2022). Furthermore, John Dough needs to have a good strict access policy, hardware maintenance, and conduct regular software updates (Ashtari, 2022).

Information Security - Protecting information such as their consumer's personal information, financial information, and intellectual property is especially important in reaching their 5-year goal earlier. John Dough needs to have security implemented in data handling, incident management access control, etc. (Fruhlinger, 2020). Furthermore, having employees trained and making sure they understand their role in protecting this information (Fruhlinger, 2020).

People security – Employees are going to be vital for the success of John Dough Pizza so need to have the right people in business for further growth. John Dough needs to implement employee security where they have training for security policies like multi-factor

authentication, background checks of employees, and business monitoring (Biswas, 2021).

Infrastructure security – While John Dough Pizza is growing, having a secure infrastructure is also especially important in the future. John Dough needs to conduct a network vulnerability assessment, secure endpoints, intrusion detection, and prevention system plan as well as have a disaster recovery plan in case there is a disaster like the one John Dough experienced before (Agency & Directorate, 2022).

Software security – John Dough software application is important since their ordering system relies on the software so conducting regular software assessments, and regular updates on the software. Also having strict access to software policies and who can manage this program (Coe, 2021). John Dough also needs to have an incident response plan if there are software issues certain authorities can be contacted to handle the situation effectively and promptly, so it doesn't affect the business operations (Coe, 2021).

John Dough Pizza has a 5-year goal of Growing the business into remote geographic environments, delivering franchisees with innovative pizza ordering and management systems, and becoming the #1 name in online pizza ordering through social media engagement and activities. To achieve these goals John Dough would need to achieve the small tasks first like having a business plan, and adequate infrastructure to expand into all remote geographic environments. Implementing an ordering system that uses authentication to understand fraudulent orders while protecting customer information. Using social media as a tool to bring in competition and prizes to customers to encourage them to take part and engage with customers can start building customer loyalty which will help John Dough in the future.

REFERENCES

Agency, N. S., & Directorate, C. (2022). (rep.). *Network Infrastructure Security Guide* (OO, Vol. U, Ser. 118623-22, pp. 2–28). San Jose, California: Cisco Systems.

Ashtari, H. (2022, January 4). *What is hardware security? definition, threats, and best practices*. Spiceworks. Retrieved May 8, 2023, from https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-hardware-security/

Belding, G. (2019, December 23). *NIST CSF: The seven-step cybersecurity framework process*. Infosec Resources. https://resources.infosecinstitute.com/topic/nist-csf-the-seven-step-cybersecurity-framework-process/

Biswas, S. (2021, December 16). *What is continuous background screening? definition and key considerations for deployment*. Spiceworks. Retrieved May 8, 2023, from https://www.spiceworks.com/hr/recruitment-onboarding/articles/what-is-continuous-background-screening/

Center for Internet Security. (2023). *The 18 CIS Controls*. CIS. https://www.cisecurity.org/controls/cis-controls-list

Coe, F. (2021, May 19). *What is software security and why is it important?* Contentful. Retrieved May 8, 2023, from https://www.contentful.com/blog/software-security-to-deliver-digital-experiences-fast/

Fruhlinger, J. (2020, January 17). *What is information security? definition, principles, and jobs*. CSO Online. Retrieved May 8, 2023, from https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

Howard, J., & Key Note Publications. (2002). IT Security. Key Note Publications.

International Organization for Standardization/International Electrotechnical Commission. (2013). ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements.

Organ, C., & Bottorff, C. (2022, March 23). *Work breakdown structure (WBS) in Project Management*. Forbes. https://www.forbes.com/advisor/business/what-is-work-breakdown-structure/

Taylor, A. (2013). Information Security Management Principles. BCS, The Chartered Institute for IT.

Whitman, M. E., & Mattford, H. J. (2019). Management of information security. Cengage Learning.

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program*. https://doi.org/10.6028/nist.sp.800-50

APPENDICES

The following are the table and flowcharts used.

CHANGE HISTORY

Date	Version	Edited By	Description of Change
19/04/2023	1.0	Lovya	Added the headings and the format of tables needed.
19/04/2023	1.1	Lovya	Added the assets in asset identification table
20/04/2023	1.2	Ishita	Edited the assets
20/04/2023	1.3	Manoj	Edited the assets
21/04/2023	1.4	Lovya	Added WFA
22/04/2023	1.5	Manoj	Edited WFA
22/04/2023	1.6	Ishita	Edited WFA
23/04/2023	1.7	Lovya	Edited WFA
24/04/2023	1.8	Lovya	Added risk assessment table
25/04/2023	1.9	Ishita	Calculated the risk rating
25/04/2023	2.0	Manoj	Edited the Risk assessment
26/04/2023	2.1	Manoj	Added the risks
27/04/2023	2.2	Lovya	Edited the risks
27/04/2023	2.3	Lovya	Added the risk controls
28/04/2023	2.4	Manoj	Added the WBS
29/04/2023	2.5	Manoj	Added the WBS flowchart
30/04/2023	2.6	Lovya	Edited WBS and flowchart
1/05/2023	2.7	Manoj	Added compliance
1/05/2023	2.8	Ishita	Edited Compliance
2/05/2023	2.9	Lovya	Edited Compliance
3/05/2023	3.0	Ishita	Added introduction and scope
4/05/2023	3.1	Lovya	Added assumptions, executive summary.
5/05/2023	3.2	Manoj	Added future programs
6/05/2023	3.3	Lovya	Added references.
6/05/2023	3.4	Manoj	Added references
7/05/2023	3.5	Lovya	Formatted the document
8/05/2023	3.6	Manoj	Added the cover page
9/05/2023	3.7	Lovya	Added table of contents.

10/05/23	3.8	Ishita, Manoj, Lovya	Made some last changes.

CHANGE CONTRIBUTION

Group Member	Tasks	Contribution	Comments
Lovya Bajaj	Risk Identification and assessment, Added WFA criteria and weighting, Added the risk controls, Edited WBS and flowchart	40% - Overall helpful in delegating tasks and doing the work. Helpful with questions asked	n/a
Ishita Chopra	Calculated the risk rating, added introduction and scope, Edited the assets and risks.	25% - Did their assigned task and helped with editing the document	n/a
Manoj Bhandari	Added the risks, edited control description, added future programs, added the WBS flowchart, edited assets	35% - Did their part and helped with editing the document as well.	n/a
Chamidu DALAMADAGEDARA	N/A	0%	Didn't reply to any emails and didn't contact in anyway.

[i]