

Student: Carrick Blake

Course: CYBR 3300 Semester: FL 2025

	Asset Name	Brief Asset Description	Asset Location	Data Owner	Type of Data	RTO	RPO	Importance	Source	Destination	# of Users
1	Active Directory Service	Service for Microsoft Windows, that functions as a centralized directory service.	Server A - Data Cen	Celica Thomp	CC	2: 8 hours	1: 4 hours	Critically Important	From Microsoft	All computers using this	26
2	Active Directory SQL DB	Database that stores information for MS AD.	Server A - Data Cen	Celica Thomp	CC	2: 8 hours	1: 4 hours	Critically Important	From Active Directory	Devices pulling informat	3
3	Primary DNS	The company network's DNS, which translates human-readable domain names into machine-readable IP addresses.	Server B - Data Cen	Celica Thomp	CC	0: 30 min	1: 4 hours	Critically Important	From Cat6-backbone	All users that are on the	26
4	DNS Database	Stores the Primary Domain Name Service's records and information.	Server B - Data Cen	Celica Thomp	CC	0: 30 min	1: 4 hours	Very Important	From the Domain Name Back to the Domain Name		3
5	Cat6-backbone Network	The company's network.	Routers within the D	Celica Thomp	CC, PII, PCI	0: 30 min	1: 4 hours	Very Important	From the routers withi	All devices connected to	26
6	Email Database	Database for all company email information.	Server C - Data Cen	Celica Thomp	CC, PCI	2: 8 hours	3: 1 day	Very Important	From Microsoft	To all employees in the	3
7	ase Accounting Software	Accounting software that provides accounting services such as Payroll and General Ledger.	Server D - Data Cen	Morgan Lee	CC, PCI, PII	3: 24 hou	2: 8 hours	Very Important	From Traverse	To the accounting depa	6
8	Accounting SQL DB	Database that stores the information for the Traverse Accounting Software.	Server D - Data Cen	Morgan Lee	CC, PII, PCI	3: 24 hou	3: 1 day	Very Important	From the need to store	To the accounting depa	6
9	se Distribution Software	Distribution software that provides distribution services such as inventory management, warehouse management, and requirements planning.	Server E - Data Cen	Vicki Webb	CC	3: 24 hou	2: 8 hours	Very Important	From Traverse	To distribution manager	5
10	Distribution SQL DB	Database that stores all information related to distribution	Server E - Data Cen	Vicki Webb	CC	3: 24 hou	2: 8 hours	Very Important	From the need to store	To the distributing depa	5
11	Traverse ERP Software	Provides Web Portals for the ecommerce website, and customer relationship management	Server F - Data Cen	Taylor Brooks		1: 1 hour	1: 4 hours	Important	From Traverse	To the sales and purcha	9
12	ERP SQL DB	The database for the ERP software	Server F - Data Cen	Taylor Brooks	CC, PII	1: 1 hour	1: 4 hours	Important	From the need to store	To the ERP software.	9
13	prk attached storage #1	Provides a weekly backup for all of Rack 1 servers' databases.	Dell Storage NX 3xx	Celica Thomp	CC, PCI, PII	5: 1 week	5: 1 week	Important	From Dell	To all servers in need of	3
14	Office 365 DB	Database for microsoft 365	Server G - Data Cen	Celica Thomp	CC	3: 24 hou	4: 2 days	Important	From information bein	To all office computers t	26
15	st Information Server #1	Information server that contains Intranet support, but more importantly stores web document and data such as internal forums.	Server H - Data Cen	Celica Thomp	CC	4: 2 days	4: 2 days	Important	From the need to post	To all employees that ne	26
16	Optimum HRIS	Provides payroll management, human resources services, and time tracking for employees.	Server I - Data Cen	Melinda Hixor	CC, PII, PCI	1: 1 hour	1: 4 hours	Important	From Optimum	To the Human Resource	4
17	HRIS DB	The database for Optimum HRIS	Server I - Data Cen	Melinda Hixor	CC, PII, PCI	1: 1 hour	1: 4 hours	Important	From the need to store	To the Human Resource	4
18	st Information Server #2	Provides web filtering and proxy services, contains Intranet DB.	Server K - Data Cen	Celica Thomp	CC	1: 1 hour	3: 1 day	Somewhat Importan	From SupportIT, Fore	To the IP department.	3
19	SupportIT DB	Database of the IT management system, which contains information on system configurations, updates, and helpdesk tickets.	Server K - Data Cen	Celica Thomp	CC	3: 24 hou	3: 1 day	Somewhat Importan	From the need to store	To the SupportIT system	3
20	prk attached storage #2	Provides a weekly backup for all of Rack 2 servers' databases.	Dell Storage NX 3xx	Celica Thomp	CC, PII, PCI	5: 1 week		Somewhat Importan	From Dell	To all servers in need of	3

Note: Once you enter the assets here, they will autopopulate throughout the spreadsheet.

Student: Carrick Blake Course: CYBR 3300 Semester: FL 2025

Decision Matrix for Asset Valuation							
	Criteria ➡	Likelihood	Operational Impact	Financial Impact			
	Criteria weights ➡						
#	Information Asset ↓	0.4	0.3	0.3		TOTAL (1.0)	Importance
6	Accounting SQL DB	5	3	5		4.4	Critically Important
17	HRIS DB	4	4	5		4.3	Critically Important
12	ERP SQL DB	5	2	5		4.1	Critically Important
13	Network attached storage #1	5	1	5		3.8	Very Important
20	Network attached storage #2	5	1	5		3.8	Very Important
3	1GbE Cat6-backbone Network	4	5	2		3.7	Very Important
1	Active Directory Service	3	4	4		3.6	Very Important
2	Active Directory SQL DB	3	4	4		3.6	Very Important
5	Traverse Accounting Software	5	2	3		3.5	Very Important
16	Optimum HRIS	2	4	5		3.5	Very Important
9	Primary DNS	3	5	1		3	Important
10	DNS Database	3	5	1		3	Important
7	Traverse Distribution Software	2	4	3		2.9	Important
8	Distribution SQL DB	2	4	3		2.9	Important
18	Internet Information Server #2	3	3	1		2.4	Important
4	Email Database	2	4	1		2.3	Important
19	SupportIT DB	3	2	1		2.1	Important
14	Office 365 DB	1	3	1		1.6	Somewhat Important
15	Internet Information Server #1	2	1	1		1.4	Somewhat Important
11	Traverse ERP Software	1	2	1		1.3	Somewhat Important

CRITERIA JUSTIFICATION (Replace blanks with your own content)

- Criterion 1 I chose likelihood because how often this information asset is threatened, I find to be one of the more important factors to consider. A weight of 0.4 was selected for this criterion because if the specific asset is widely known to be a target, it is important to be more concerned with it.
- Criterion 2 I chose Operational Impact because how much this impacts the company, aside from finance, is also something important to consider. A weight of 0.3 was selected for this criterion because depending on the amount of disruption that data loss in this asset causes the more of a problem the company would have.
- Criterion 3 I chose Financial Impact because regardless of the asset there is some sort of financial loss in some way. A weight of 0.3 was selected for this criterion because financial impact is potentially the most considered factor in risk assessments.

If you choose fewer than 5 criteria, delete unneeded rows and ensure totals works.

Select your own and use realistic values  
Replace all information not in bold with your own values  
Scales for Criterion weights are 0-1.00 (usually in increments of .05-.10)  
Scales for Criterion values (cells) are 0-5 (usually in increments of 1)  
0 is lowest, 5.0 is the highest, in .1 increments

Your last step is to sort all assets by the TOTAL column.  
Be sure you only sort columns B4 through I33 (or whatever number of assets you end up with).  
You want to leave the number column in order such that your number 1 asset is listed by the number 1.

Use the following scale to convert the weighted table analysis "Total" values to Clearwater "Importance" scores:  
Don't change the values below, they're used in the table.

0	1 Not Important
1.01	2 Somewhat Important
2.01	3 Important
3.01	4 Very Important
4.01	5 Critically Important

The TOTAL column's calculations are based on 5 criteria. If you use more or less, you will need to add/remove rows and adjust the calculations.

Student: Carrick Blake  
Org Risk Threshold

Course: CYBR 330C Semester: FL 2025

10

Enter a value between 0 (we accept all risk) and 25 (we accept no risk) - the average organization is between 7-12.

	Assets	Policy	IR/DR Plan	Employee Training	Data Backup Plan	Redundant Server	Likelihood	Impact	Risk	Risk Notes: I selected this risk likelihood value because _____. I selected this risk impact value because _____.
1	Active Directory Service	Yes	Yes	Yes	Yes	Yes	3	4	12	I selected this risk likelihood value because Active Directory attacks are becoming very common. I selected this risk impact value because the active directory service contains crucial privileges.
2	Active Directory SQL DB	In-Progress	In-Progress	In-Progress	Yes	Yes	3	4	12	I selected this risk likelihood value because active directory attacks are becoming very common. I selected this risk impact value because the active directory databases are relatively targetted for containing authentication information.
3	1GbE Cat6-backbone Network	Yes	Yes	In-Progress	No	No	4	4	16	I selected this risk likelihood value because network attacks are very common. I selected this risk impact value because the information that is sent over the network has varying value and sensitivity.
4	Email Database	In-Progress	In-Progress	In-Progress	Yes	Yes	2	3	6	I selected this risk likelihood value because attackers would only seek out an email database for basic personal info. I selected this risk impact value because the most impact that an attack on this database would have would be a data leak, which can be severe depending on how much is stored here.
5	Traverse Accounting Software	Yes	Yes	Yes	Yes	Yes	5	3	15	I selected this risk likelihood value because the most common motive for attackers is financial gain. I selected this risk impact value because this software is crucial to all employees and banking.
6	Accounting SQL DB	In-Progress	In-Progress	In-Progress	Yes	Yes	5	5	25	I selected this risk likelihood value because attackers seek financial gain the most. I selected this risk impact value because a data leak of this information would be disastrous for the company.
7	Traverse Distribution Software	Yes	Yes	Yes	Yes	Yes	2	4	8	I selected this risk likelihood value because distribution software is attacked commonly, but not as common as the other services that this company has. I selected this risk impact value because it impacts such a vast amount of the company.
8	Distribution SQL DB	In-Progress	In-Progress	In-Progress	Yes	Yes	2	4	8	I selected this risk likelihood value because a distribution database does not seem like it would be as likely to be attacked compared to the other databases. I selected this risk impact value because the distribution database impacts a large span of the company.
9	Primary DNS	Yes	Yes	No	Yes	Yes	3	3	9	I selected this risk likelihood value because the majority of organizations face DNS attacks yearly. I selected this risk impact value because while there isn't sensitive information to be leaked, if the internet malfunctions there is a large operational impact.
10	DNS Database	Yes	Yes	Yes	Yes	Yes	3	3	9	I selected this risk likelihood value because a DNS attack is common for larger organizations like this one. I selected this risk impact value because there is a little bit of infrastructure information that the company would not want to be leaked.
11	Traverse ERP Software	Yes	Yes	Yes	Yes	Yes	1	2	2	I selected this risk likelihood value because the actual ERP software is not something that attackers would seek, but potentially use as a vector. I selected this risk impact value because the software by itself would not sensitive information, however if the ecommerce site is down there is a bit of impact.
12	ERP SQL DB	In-Progress	In-Progress	In-Progress	Yes	Yes	5	5	25	I selected this risk likelihood value because this is what attackers would be seeking the most to find, as it has customer payment information. I selected this risk impact value because it contains information that would be incredibly costly to the company if it were leaked.

Student: Carrick Blake  
Org Risk Threshold

Course: CYBR 330C Semester: FL 2025  
10 Enter a value between 0 (we accept all risk) and 25 (we accept no risk) - the average organization is between 7-12.

	Assets	Policy	IR/DR Plan	Employee Training	Data Backup Plan	Redundant Server	Likelihood	Impact	Risk	Risk Notes: I selected this risk likelihood value because _____. I selected this risk impact value because _____.
13	Network attached storage #1	In-Progress	In-Progress	Yes	Yes	No	5	5	25	I selected this risk likelihood value because backups are heavily targeted by attackers since this contains all of the information that an attacker could ever seek. I selected this risk impact value because this has all of the information that the company would not want to be leaked, as it has customer payment information, accounting information, and more.
14	Office 365 DB	In-Progress	In-Progress	Yes	Yes	Yes	1	1	1	I selected this risk likelihood value because attackers would not care for Microsoft office information, unless they were wanting to disrupt the plans of this company. I selected this risk impact value because the information contained in here would not be really detrimental to the company if it were leaked.
15	Internet Information Server #1	Yes	Yes	Yes	Yes	Yes	2	2	4	I selected this risk likelihood value because a intranet service, while it is targeted by elite hackers, it isn't common to be attacked by novice attackers. I selected this risk impact value because there is only information that minorly impacts the company here, and the services on here are not crucial.
16	Optimum HRIS	Yes	Yes	Yes	Yes	Yes	4	5	20	I selected this risk likelihood value because attackers would be searching for the very sensitive information that can be found here. I selected this risk impact value because if the the human resource service is something that the company could not afford to have offline for an extended period of time, due to it tracking employee time.
17	HRIS DB	In-Progress	In-Progress	In-Progress	Yes	Yes	4	5	20	I selected this risk likelihood value because attackers seek information that human resource databases hold. I selected this risk impact value because the information stored here would be incredibly costly if it were leaked, as it contains all employee info.
18	Internet Information Server #2	Yes	Yes	Yes	Yes	Yes	3	2	6	I selected this risk likelihood value because Forefront TMG has vulnerabilities that can be used as an attack vector. I selected this risk impact value because having this gateway attacked itself would only have a bit of operational impact on the company.
19	SupportIT DB	In-Progress	In-Progress	In-Progress	Yes	Yes	3	2	6	I selected this risk likelihood value because the information stored here contains information about all devices across the company, which an attacker would probably seek for Privilege Escalation. I selected this risk impact value because having device information be leaked could be problematic, however by itself it is not as impactful as the other devices.
20	Network attached storage #2	Yes	Yes	Yes	Yes	No	5	5	25	I selected this risk likelihood value because attackers would seek access to a backup like this since it contains all human resource information including previous employees. I selected this risk impact value because if this information was leaked it would be incredibly costly to the company.

Student: Carrick Blake Course: CYBR 3300 Semester: FL 2025

	Org Risk Threshold	10		Risk Controls							
	Assets	Current Risk	Risk Treatment	Policy	IR/DR Plan	Employee Training	Data Backup Plan	Redundant Server	New Likelihood	New Impact	Projected Risk
1	Active Directory Service	12	Mitigate	Enhance	Enhance	Add	Enhance	Enhance	2	2	4
2	Active Directory SQL DB	12	Mitigate	Add	Add	Add	Enhance	Enhance	2	2	4
3	1GbE Cat6-backbone Network	16	Mitigate	Enhance	Enhance	Enhance	Add	Add	3	2	6
4	Email Database	6	Avoid	Add	Add	Add	Enhance	Enhance	1	1	1
5	Traverse Accounting Software	15	Mitigate	Enhance	Enhance	Enhance	Enhance	Enhance	3	2	6
6	Accounting SQL DB	25	Mitigate	Add	Add	Add	Enhance	Enhance	4	2	8
7	Traverse Distribution Software	8	Accept	Enhance	Enhance	Enhance	Enhance	Enhance	2	2	4
8	Distribution SQL DB	8	Accept	Add	Add	Add	Enhance	Enhance	2	2	4
9	Primary DNS	9	Accept	Enhance	Enhance	Add	Enhance	Enhance	2	2	4
10	DNS Database	9	Mitigate	Enhance	Enhance	Enhance	Enhance	Enhance	1	2	2
11	Traverse ERP Software	2	Accept	Enhance	Enhance	Enhance	Enhance	Enhance	3	1	3
12	ERP SQL DB	25	Mitigate	Add	Add	Add	Enhance	Enhance	3	3	9

**Risk Notes:**  
 I selected this new risk likelihood value because \_\_\_\_\_.  
 I selected this new risk impact value because \_\_\_\_\_.  
 I selected this new risk likelihood as it would still be common for Active Directory attacks to be attempted, but if properly secured it wouldn't be become an attack. I selected this new impact value because if we secured all of the information that the active directory service accesses, the impact would go down dramatically  
 I selected this new risk likelihood as it would still be common for Active Directory attacks to be attempted, especially on this database, but with proper database security, the chances of an actual incident occurring would be low. I selected this new impact value because if we secured all of this information stored, and strongly encrypted all of the credentials that Active Directory accesses, the impact would be reduced heavily.  
 I selected this new risk likelihood due to the fact that network attacks are very difficult to control the likelihood of occurring themselves, as it's one of the most popular vectors aside from Phishing. I chose this new risk impact value because with solid security in the network, and encryption for all protocols, attackers would not be able to use the information they receive well.  
 I chose this new risk likelihood because if all security controls were in place, this database would be secured thoroughly to the point that attackers would probably not bother. I selected this new impact value because if all this database contains was undecryptable email information, the company would not face much of an impact.  
 I selected this new risk likelihood because accounting software would still be a big target within the company, but with proper training and policy the chances of anything occurring to this software would decrease. The new impact value is at 2 as with all controls involved it would be recoverable if there was an incident.  
 I chose this new risk likelihood because an accounting database regardless of how secure will have incidents being such a highly targetted asset. I chose this new impact value as if the database was thoroughly encrypted, protecting all payroll and banking information, the impact would not be too severe.  
 I chose this new risk likelihood as if this distribution software had strong controls, it would not be used as a vector by any threat. I chose this new risk likelihood because if there was an incident, we would not be storing any sensitive information on this software due to proper employee training.  
 I chose this new risk likelihood as after implementing all controls to protect a database like this , a distribution software database would not be worth the cost to attackers. I chose this new risk impact value because if all controls were in place there wouldn't be much harm that this information getting leaked would do. Especially if it was encrypted.  
 I chose this new risk likelihood because after all controls being in place, there are still chances of having a DNS attack, but it would be less likely. I chose this new risk impact because if employees are properly trained to recognize when they are on a malicious site, the impact would be minimal.  
 I chose this risk likelihood as the chances of having the DNS database itself being attacked after all security controls are in place would be pretty minimal. I chose this risk impact value because the amount of damage that would be done with this information getting out would be minimal, since it's not as sensitive as employee or customer PII.  
 I chose this new risk likelihood because the likelihood of the software itself having an incident is still pretty high, as it's the ecommerce service. I chose this new risk impact because after implementing all controls there would not be crucial information stored in this service.  
 I chose this new risk likelihood because a database with payment information regardless of how secure will have incidents being such a highly targetted asset. I chose this new impact value as if the database was thoroughly encrypted, protecting all payroll customer payment information thoroughly, the impact would not be too severe.

Student: Carrick Blake Course: CYBR 3300 Semester: FL 2025

	Org Risk Threshold	10		Risk Controls							
	Assets	Current Risk	Risk Treatment	Policy	IR/DR Plan	Employee Training	Data Backup Plan	Redundant Server	New Likelihood	New Impact	Projected Risk
13	Network attached storage #1	25	Transfer	Add	Add	Add	Add	Add	3	3	9
14	Office 365 DB	1	Accept	Enhance	Enhance	Enhance	Enhance	Enhance	1	1	1
15	Internet Information Server #1	4	Accept	Enhance	Enhance	Enhance	Enhance	Enhance	2	1	2
16	Optimum HRIS	20	Mitigate	Enhance	Enhance	Enhance	Enhance	Enhance	4	2	8
17	HRIS DB	20	Mitigate	Add	Add	Add	Enhance	Enhance	4	2	8
18	Internet Information Server #2	6	Accept	Enhance	Enhance	Enhance	Enhance	Enhance	2	2	4
19	SupportIT DB	6	Avoid	Add	Add	Add	Enhance	Enhance	2	2	4
20	Network attached storage #2	25	Transfer	Add	Add	Add	Add	Add	3	3	9

**Risk Notes:**

I selected this new risk likelihood value because \_\_\_\_\_.

I selected this new risk impact value because \_\_\_\_\_.

I chose this new risk likelihood because backups are very commonly targetted assets, since they store all information an attacker would ever want, but with proper training and controls in place the chances of having an incident with the backup alone would not be extremely common. I chose this new risk impact because the information on here would still be bad if it was released to the public, but having controls in place on all databases it would be mitigated.

I chose this new risk likelihood because a threat actor would not care much about a Microsoft 365 database unless it was known to store incredibly sensitive information. However since this information is stored in the other databases throughout the Data Center this would also make the risk impact low.

I chose this new risk likelihood as if properly secured, incidents occurring with an internal forum would be uncommon. I chose this new risk impact because the information that should only be stored on this after controls being in place would be basic employee question and answer information. Which would not do much harm to the company if it were released.

I chose this new risk likelihood because being a human resources software, and potentially containing SPII it would be a big target for threat actors regardless of how many controls were in place. I chose this risk impact because if all of the information going across this software was properly handled, and encrypted. There would not be much of an impact.

I chose this new risk likelihood because with this being a human resources database, it is guaranteed to contain employee SPII, and incidents are sure to occur. I chose this new risk impact because if properly secured and encrypted it would not harm the company heavily if it were leaked.

I chose this new risk likelihood because Forefront TMG, would still have security vulnerabilities, but assuming the company found a more robust service to replace TMG, the likelihood would go down heavily. I chose this new risk impact because the information that could be leaked from this would not be harmful to the company especially after controls were in place.

I chose this new risk likelihood because if properly secured the IT ticketing system should not have incidents commonly, and it would not be a popular vector. I chose this new risk impact value because while it does contain information about the devices that the company uses, if the database itself was properly secured and encrypted it would not be detrimental to the company.

I chose this new risk likelihood because backups are very commonly targetted assets, since they store all information an attacker would ever want, but with proper training and controls in place the chances of having an incident with the backup alone would not be extremely common. I chose this new risk impact because the information on here would still be bad if it was released to the public, but having controls in place on all databases it would be mitigated.