Instructions

Each phase of this Risk Assessment project is designed to take you through the exact same tasks an individual conducting a risk management program for an organization would perform. Begin by reading through these instructions.

PART 1 –INFORMATION ASSET INVENTORY AND PRIORITIZATION

Use the case organization document to complete Tables 1 and 2 with the information assets you identify.

TABLE 1 - LISTING OF INFORMATION ASSETS

Complete Table 1 below specifying between 20-25 information assets appropriate to the case not provided (add/remove rows as needed), based on assumptions you derive from the case document.

Data Owner: *refer to the text for the definition of the data owner. While the CIO may be the data custodian, he/she is most likely NOT the owner of non-IT data.*

Type of Sensitive Data Options:

- *Customer Confidential (Conf) – any data retained by the organization that has been labeled as confidential – i.e. limited in its access, distribution and use. Examples include executive meeting records; marketing and strategic plans not yet released; details of communications with and services provided to select client organizations; and company IT and InfoSec program details.*
- *Electronic Patient Healthcare Information (ePHI) – any data retained by the organization that contains personal medical information, including that of employees and clients. Employee health coverage information in an HR file is not ePHI for our purposes – unless it included details on the coverage such as the account number, primary care physician, etc. Most HR records would only contain the name of the coverage (e.g. Blue Cross/Blue Shield HMO), but not the details.*
- *Payment Card Information (PCI) – any data retained by the organization that contains payment card information such as debit/credit card numbers with expiration dates, users' names, security codes and/or billing information.*
- *Personally Identifiable Information (PII) – any data retained by the organization that contains personally identifiable information that could be used to identify an individual (or steal their identity) including names with social security numbers, driver's license numbers, addresses, phone numbers, family members.*
- *Student Records (FERPA) – any data retained by the organization that contains academic information regarding an individual including names with student numbers, social security numbers, courses taken, grades assigned, academic integrity/misconduct issues, financial aid and/or other PII.*

A few Assets have been added to the table to help you get started. You will need to identify the rest on your own. Add rows as needed.

Table 1: Listing of Information Assets for *Case Organization*

Asset	Data Owner	Type of Sensitive Data
1) **Active Directory Server (Server A)**	CIO	**Stores employee/user accounts, usernames, passwords, login credentials all personally identifiable.**
2) AD SQL DATABASE	CIO	**Backend for AD server. Contains metadata, access permissions, group memberships linked to user identities.**
3) DNS Server B	CIO	**Resolves hostnames to IPs. No business-critical or sensitive data stored.**
4) DNS SQL DB	CIO	**DNS cache and query logs. May be reviewed for security audits but contains no PII or PCI.**
5) Exchange Email Server (Server C)	CIO	Sends/receives email often contains employee info, internal discussions, customer communications.
6) Email Database	CIO	Stores historical messages may contain contracts, customer records, sensitive attachments.
7) Traverse Accounting Software	CFO	Used for payroll, vendor billing, tax reports. Deals with credit card info, SSNs, bank details.
8) Accounting SQL Database	CFO	Stores account numbers, payment transactions, vendor/customer payment info.
9) Traverse Distribution Software	COO	Contains pricing, shipping, supplier info strategic operational data not publicly shared.
10) Distribution SQL Database	COO	Holds logistics data, warehouse inventories, partner shipping schedules.
11) Traverse ERP Software	COO	Handles business-wide operations like customer orders, portals, financials.
12) **ERP SQL Database**	CIO	Database stores ecommerce orders, customer info, payment details, user credentials.
13) Web Portals (TERP-Web)	Sales Manager	Online access for customers and partners; handles logins, order forms, payment info.
14) CRM Application (TERP-CRM)	Sales Manager	Customer profiles: emails, names, purchase history, payment info, contact details.
15) **HRIS Software**	HR Manager	HR data: names, addresses, health plans, benefits, time/attendance, payroll interface.

Asset	Data Owner	Type of Sensitive Data
16) HRIS SQL Database	HR Manager	Detailed employee records and private health/benefits info. Sensitive under HIPAA-like standards.
17) Office 365 Server	CIO	Hosts internal docs, spreadsheets, policies, plans many classified “internal use only.”
18) Office 365 DB	CIO	Database of user documents, internal comms, schedules not public, business-critical.
19) Internet Information Server (IIS)	CIO	Hosts internal wikis, documentation, HR policies. Not exposed externally but still sensitive.
20) Forefront TMG Server	CIO	Filters web traffic; logs user behavior. May contain URLs visited, attempts to access blocked sites.
21) SupportIT Application	IT Manager	Used for ticketing, configurations, internal system data valuable for IT audits.
22) SupportIT DB	IT Manager	Logs system health, user problems, asset configs internal IT tool used for incident response.
23) **NAS1 (Backup for Rack 1)**	CIO	Stores backups of servers A–F (AD, email, accounting). Indirectly holds all Rack 1 sensitive data.
24) **NAS2 (Backup for Rack 2)**	CIO	Backs up HRIS, ERP, CRM, and more contains highly sensitive data including health and customer info.
25) Enigmeh AES Encryption Software	CIO	Controls access to all sensitive data; encryption keys protect the confidentiality of stored information.

TABLE 2 – WEIGHTED RANKING OF INFORMATION ASSETS

Instructions for Table 2.
Create a weighted table analysis, as described in a previous lecture, to rank all information assets from Table 1.

1. *Identify 4-5 criteria you will use to evaluate the assets identified earlier and assign weights to the criteria. Note the weights must sum to 1.0 (as in 100%).*
2. *Copy the complete list of assets from Table 1 into the first column of Table 2.*
3. *Evaluate each information asset against your criteria by assigning a value of 0 to 5 (with 5 being most critical) under each asset criterion. Use the following scale in your assignments, to answer the question: "How important is this asset with regard to this criterion?"*
    a. *5 - Critically important*
    b. *4 - Very important*
    c. *3 - Important*
    d. *2 - Somewhat important*
    e. *1 - A little important*
    f. *0 - Not important*
4. *Perform the calculations to determine the totals. (each cell is multiplied by its criterion's weight, then all products are summed into the total column).*
   Note: sample criteria weights were added to the table to illustrate function (e.g. Crit 1; .20). Replace these values with your own criteria and weights.
5. *Finally sort the entire table on the Total column. When you're finished, your number one asset (first on the list) should be the one with the largest total, and thus the highest importance.*

Table 2: Weighted Ranking of Information Assets

Criteria ➔	***Business Impact*** ***Critical systems that, if lost, halt operations or cost millions***	***Data Sensibility*** ***More sensitive data = greater compliance and reputational risk***	***Dependency*** ***Is this a prerequisite for other systems to work?***	***Recovery Complexity*** ***How hard/time-consuming to restore or recover?***	***Access Exposure*** ***Is this exposed to internal/external access (attack surface)?***	**Total** ***0-5.0***
Criteria Weight➔ **➘Asset Name**	***0.30***	***0.25***	***0.20***	***0.15***	***0.10***	
1) NAS 2	*5*	*5*	*5*	*5*	*2*	*4.70*
2) NAS 1	5	5	5	5	2	4.70
3) Traverse ERP Software	5	5	5	4	3	4.65
4) ERP SQL Database	5	5	5	4	3	4,65
5) HRIS SQL Database	5	5	4	4	2	4.35
6) HRIS Software	5	5	4	4	2	4.35
7) Traverse Accounting Software	5	5	4	4	2	4.35
8) Accounting SQL Database	5	5	4	4	2	4.35
9) Active Directory Server	5	4	5	3	3	4.25
10) AD SQL Database	5	4	5	3	3	4.25
11) Enigmeh AES Encryption Software	5	5	3	4	2	4.15
12) Email Database	4	5	4	3	3	4.00
13) Exchange Email Server	4	4	4	3	4	3.85
14) Web Portals (TERP-Web)	4	4	4	3	4	3.85
15) CRM Application	4	4	4	3	3	3.75
16) Distribution SQL Database	4	3	3	3	2	3.20
17) Traverse Distribution Software	4	3	3	3	2	3.20
18) Office 365 Server	3	3	3	3	3	3.00
19) Office 365 Database	3	3	3	3	3	3.00

Criteria ➔	***Business Impact*** ***Critical systems that, if lost, halt operations or cost millions***	***Data Sensibility*** ***More sensitive data = greater compliance and reputational risk***	***Dependency*** ***Is this a prerequisite for other systems to work?***	***Recovery Complexity*** ***How hard/time-consuming to restore or recover?***	***Access Exposure*** ***Is this exposed to internal/external access (attack surface)?***	**Total** ***0-5.0***
Criteria Weight➔ **➘Asset Name**	***0.30***	***0.25***	***0.20***	***0.15***	***0.10***	
20) Forefront TMG Server	3	3	3	2	2	2.75
21) Internet Information Server	3	2	2	2	2	2.30
22) DNS Server	3	0	4	2	2	2.20
23) SupportIT Application	2	2	2	2	2	2.00
24) SupportIT Database	2	2	2	2	2	2.00
25) DNS SQL Database	2	0	3	2	1	1.60

Criteria Descriptions: *List and describe your criteria used in Table 2, below. Then provide a detailed justification as to how and why you selected these criteria and their weights.*

Format: Criterion (e.g. Impact on Profitability) – this criterion is defined as _____, This criterion was selected because _____, A weight of ___ was selected for this criterion because _____.

1. **Business Impact** –
This criterion is defined as the extent to which the failure, compromise, or unavailability of an asset would disrupt core business operations, reduce productivity, or cause financial loss.
This criterion was selected because assets that have a high impact on business continuity (e.g., accounting systems, ERP) are essential to daily operations and revenue generation.
A weight of **0.30** was selected for this criterion because ensuring business operations remain uninterrupted is the top priority in risk management.

2. **Data Sensitivity** –
This criterion is defined as the classification and criticality of the data processed or stored by the asset, particularly if it includes Personally Identifiable Information (PII), Payment Card Information (PCI), or Electronic Protected Health Information (ePHI).
This criterion was selected because data breaches involving sensitive data can result in legal liabilities, regulatory fines (e.g., GDPR, HIPAA), and loss of customer trust.
A weight of **0.25** was selected for this criterion because protecting sensitive data is essential to maintaining compliance and reputation.

3. **Dependency** –
This criterion is defined as the degree to which other systems, processes, or users depend on this asset to function correctly.
This criterion was selected because an asset that serves as a foundational component (e.g., DNS, Active Directory, backup servers) can create cascading failures if compromised.
A weight of **0.20** was selected for this criterion to reflect its operational importance across the IT infrastructure.

4. **Recovery Complexity** –
This criterion is defined as the difficulty and time required to restore the asset and its data to full operational status following a failure or compromise.
This criterion was selected because complex systems (e.g., multi-server applications, integrated databases) require more time and expertise to recover, increasing downtime and cost.
A weight of **0.15** was selected for this criterion because, although important, it is a secondary consideration to business impact and data sensitivity

5. **Access Exposure** –
This criterion is defined as the degree to which the asset is accessible to internal users, external parties, or exposed to the internet or public networks.
This criterion was selected because assets with broader or unsecured access surfaces are at higher risk of being targeted in cyberattacks.
A weight of **0.10** was selected for this criterion because it's critical for threat modeling but carries less weight than business function or sensitivity.

PART 2 – THREATS TO INFORMATION ASSET INVENTORY AND PRIORITIZATION

Begin by entering into the first column of Table 3 the threats to the organization's information assets you expect they would encounter. You may use the list from the lectures, a list from another source, or create one on your own.

TABLE 3 – WEIGHTED RANKING OF THREATS TO INFORMATION ASSETS
Complete Table 3 below specifying any threats to information assets appropriate to the case not provided (add/remove rows as needed), based on assumptions you derive from the case document. Next rank order the threats from most to least dangerous based on criteria you select.

A few Threats have been added to the table to help you get started. You will need to identify the rest on your own. Add rows as needed.

Next, Complete the weighted table analysis, as described in a previous lecture, to rank all threat from most to least dangerous.

1. *Identify 4-5 criteria you will use to evaluate the threats and assign weights to the criteria. Note the weights must sum to 1.0 (as in 100%).*
2. *Evaluate each threat against your criteria by assigning a value of 0 to 5 (with 5 being most dangerous) under each threat criterion. Use the following scale in your assignments, to answer the question: "How dangerous is this threat with regard to this criterion?"*
    a. *5 - Critically dangerous*
    b. *4 - Very dangerous*
    c. *3 - Dangerous*
    d. *2 - Somewhat dangerous*
    e. *1 - A little dangerous*

   f. *0 - Not dangerous*
3. *Perform the calculations to determine the totals. (each cell is multiplied by its criterion's weight, then all products are summed into the total column).*
   Note: sample criteria weights were added to the table to illustrate function (e.g. Crit 1; .20). Replace these values with your own criteria and weights.
4. *Finally sort the entire table on the Total column. When you're finished, your number one threat (first on the list) should be the one with the largest total, and thus the most dangerous.*

Table 2: Weighted Ranking of Threats to Information Assets

Criteria ➔	***Impact Severity***	***Likelihood***	***Detectability***	***Recovery Cost***	***Propagation Speed***	**Total *0-5.0***
Criteria Weight➔ ⬇Asset Name	***0.30***	***0.25***	***0.15***	***0.20***	***0.10***	
1) Forces of Nature	*5*	*2*	*5*	*4*	*1*	*3.65*
2) Software Attacks	3	4	3	3	4	3.35
3) Information Extortion	5	3	2	4	4	3.65
4) Phishing / Social Engineering	4	5	3	4	4	4.10
5) Ransomware Attack	5	4	2	5	3	4.10
6) Natural Disaster (Fire/Flood)	5	2	5	4	1	3.65
7) Data Theft / Leakage	5	3	2	4	3	3.65
8) Supply Chain Attack	5	2	4	4	2	3.60
9) Denial of Service (DoS)	3	4	4	3	5	3.60
10) Unauthorized Access	4	3	3	4	3	3.50
11) Power Outage	4	3	4	3	2	3.35
12) Software Vulnerabilities	3	4	3	3	4	3.35
13) Insider Threat	4	3	2	3	3	3.15
14)						
15)						
16)						
17)						
18)						
19)						
20)						

Criteria Descriptions: *List and describe your criteria used in Table 3, below. Then provide a detailed justification as to*

how and why you selected these criteria and their weights.

Format: Criterion (e.g. Impact on Profitability) – this criterion is defined as _____, This criterion was selected because _____, A weight of ___ was selected for this criterion because _____.

1. **Impact Severity** –
This criterion is defined as the potential damage or disruption to business operations, data, or reputation if the threat successfully exploits a vulnerability.
This criterion was selected because some threats (e.g. ransomware, natural disasters) can cause massive financial, legal, and operational harm.
A weight of **0.30** was selected for this criterion because understanding the **magnitude of impact** is the most important aspect of prioritizing threats.

2. **Likelihood** –
This criterion is defined as the probability that a specific threat will materialize based on historical data, industry trends, and the organization's exposure.
This criterion was selected because threats that are more **frequent or likely** to occur should be addressed with greater urgency.
A weight of **0.25** was selected for this criterion to reflect its **high influence** on overall risk without overpowering impact severity.

3. **Detectability** –
This criterion is defined as how easily the organization can identify or detect the threat if it occurs or is attempted.
This criterion was selected because **undetected threats** (e.g. insider threats, phishing) can persist and cause more damage.
A weight of **0.15** was selected for this criterion to represent its relevance while keeping it balanced against impact and likelihood.

4. **Recovery Cost** –
This criterion is defined as the financial, technical, and operational cost required to recover from the threat once it has occurred.
This criterion was selected because recovery from certain threats (e.g. ransomware, data breaches) can be **cost-prohibitive** and time-intensive.
A weight of **0.20** was selected for this criterion due to its direct impact on resource allocation and business continuity.

5. **Propagation Speed** –
This criterion is defined as how quickly the threat can spread within the environment or escalate its damage once initiated.
This criterion was selected because **fast-moving threats** (e.g. worms, DDoS) reduce reaction time and can amplify losses.
A weight of **0.10** was selected for this criterion because it is important, but secondary compared to impact, frequency, and cost.

PART 3 – CALCULATING RISK

Begin by copying your top five (5) information assets from Table 2 and your top five (5) threats from Table 3 into Table 4.

For each cell (e.g. Threat 1 and Asset 1) estimate the likelihood of an attack from this threat on this asset, the impact of a successful attack, and then combine the two into a risk rating, using the following scales:

Likelihood:

Value	Description	Percent Likelihood	Example
0	Not Applicable	0% likely in the next 12 months'	Will never happen
1	Rare	5% likely in the next 12 months'	May happen once every 20 years
2	Unlikely	25% likely in the next 12 months'	May happen once every 10 years
3	Moderate	50% likely in the next 12 months'	May happen once every 5 years
4	Likely	75% likely in the next 12 months'	May happen once every year
5	Almost Certain	100% likely in the next 12 months'	May happen multiple times a year

Impact:

Value	Description	Example	# of Records	Productivity Lost	Financial Impact
0	Not applicable	No impact	N/A	N/A	N/A
1	Insignificant	No interruption, no exposed data	0	0	0
2	Minor	Multi-minute interruption, no exposed data	0	2 hours	$20,000
3	Moderate	Multi-hour interruption, minor exposure of data	499	4 hours	$175,000
4	Major	One day interruption, exposure of data	5,000	8 hours	$2,000,000
5	Severe	Multi-day interruption, major exposure of sensitive data	50,000	24 hours	$20,000,000

Calculate Risk = Likelihood X Impact

TABLE 4 – LIGHTWEIGHT RISK ASSESSMENT FOR INFORMATION ASSETS

	phishing	***Ransomware***	***Natural Disaster***	***Data Theft/Lekage***	***Supply Chain Attack***
NAS 2	*L =2* *I =5* *Risk =**10***	*L =3* *I =5* *Risk =**15***	*L =3* *I =5* *Risk =**15***	*L = 3* *I =5* *Risk =**15***	*L =2* *I =4* *Risk =8*
NAS 1	*L =2* *I =5* *Risk =**10***	*L =3* *I =4* *Risk =**15***	*L =3* *I =5* *Risk =**15***	*L = 3* *I =5* *Risk =**15***	*L =2* *I =3* *Risk =**8***
Traverse ERP	*L =3* *I =4* *Risk =**12***	*L =4* *I =5* *Risk =**20***	*L =3* *I =4* *Risk =**12***	*L =4* *I =4* *Risk =**16***	*L =3* *I =3* *Risk = 9*
ERP SQL DB	*L =3* *I =4* *Risk =**12***	*L =4* *I =5* *Risk =**20***	*L =3* *I =4* *Risk =**12***	*L =4* *I =4* *Risk =**16***	*L =3* *I =3* *Risk = **9***
HRIS SQL DB	*L =2* *I =4* *Risk =**10***	*L =3* *I =4* *Risk =**15***	*L =3* *I =4* *Risk =**12***	*L =4* *I =5* *Risk =**20***	*L =2* *I =3* *Risk = **6***

Finally, color code each cell based on the following Risk Rating:

Risk Rating	***Risk Description***
21-25	***Critical***
13-20	***High***
7-12	***Moderate***
0-6	***Low***

This completes the lightweight risk assessment. You will use these tables in your presentation.