Risk assessment for a non-profit organization (Giving Joy)

Mariam Mourad 20210798

Dima Sawalmeh 20200296

What is a nonprofit organization

It’s an organization that provides public benefit by providing services and awareness. Nonprofits can take various forms, including charities, foundations, associations, and social enterprises

Organization overview

Giving Joy is Jordanian nonprofit organization. It stared as a charitable initiative that runs continuous campaigns to support the less fortunate who’s in need. They mainly collect donations and have connections with other charities to ensure that the donations reach those who need them. Their campaigns reached people locally and extended to other countries as Morocco, Syria, and Lebanon.

Risk security assessment need

Now that they have network connections with other countries they feel the need to protect and keep the donations secure, as the organization is growing more and more to ensure a comprehensive evaluation of their systems, networks, and data.

The organization’s risk appetite is medium to high and the scope of it is critical to a certain point

Assets

Assets

1. Finance wise assets.
2. Donor and Member information.
3. Reputation assets.
4. Information Technology Systems and Data.
5. Volunteers , workers and Human Resources.

1- Finance wise assets.

Includes:

- Cash and Bank Accounts.
- Donations and Grants.
- Contracts and Agreements with service providers, and partners (agreements that may involve financial commitments and grants).

2- Donor information.

it is essential to recognize the sensitivity of the donor’s information and the potential risks associated with it, they’re saved in a database that includes their:

- Personal Information.
- Financial Information (donation history , Billing information).
- Volunteering history or involvement in specific projects.

3- Reputation assets.

(non-tangible)

Includes:

-Goodwill (positive feelings and support that the organization receives from the community)

-Public perception.

-Trust in the organization.

4- Information Technology Systems and Data.

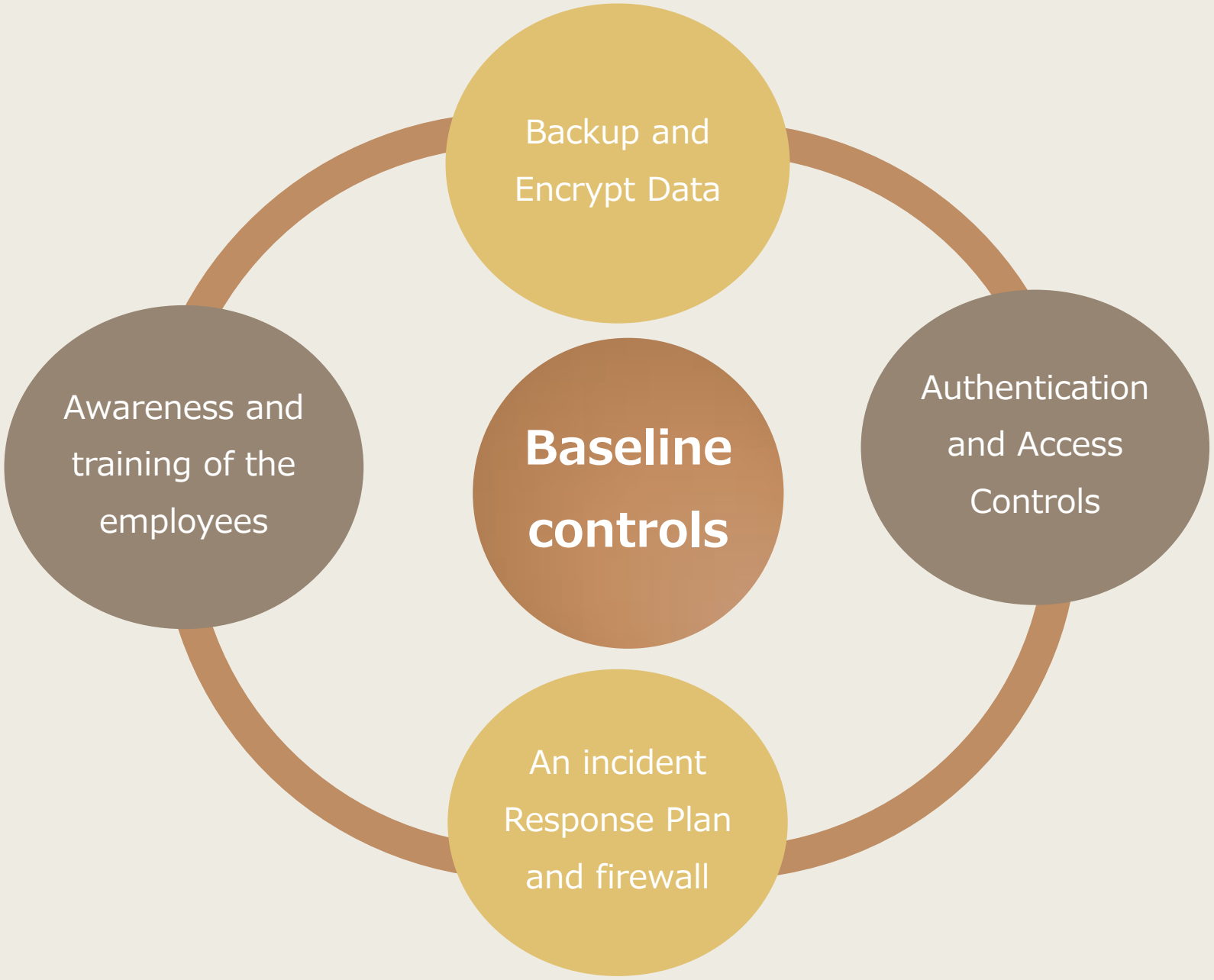
- Website , Content Management Systems and Social Media Platforms.
- Data and Document Repositories(Management of various types of data and documents).
- Network Infrastructure(Local area networks (LANs) and wide area networks (WANs) connecting the computers, devices, and servers to facilitate data sharing).
- Cloud Services and Infrastructure(cloud-based services and infrastructure, such as cloud storage, software-as-a-service (SaaS) applications).

5- Volunteers , workers and Human Resources

- Volunteer Database(containing volunteer information, such as contact details, skills, availability, and areas of interest).
- Performance Management Systems(to track and evaluate employee performance, set goals, and provide feedback).

Risk Register Table

Assets	Threats/ Vulnerability	Existing controls	Likelihood	Consequences	Risk level	Risk priority
Donor and Member Information	Data breaches, Unauthorized access, Identity theft, Sensitive information, Phishing attacks, Insider misuse of data.	Data Encryption policies, and hashing	Possible	Major	Extreme	1
Information Technology Systems and Data	Distributed Denial of Service (DDoS). Weak or easily guessable passwords. Phishing attacks. Lack of regular updates and patches for the CMS.	Layered firewalls, Authentication and Access Controls	Rare	Major	High	2
Finances	Weak Internal Controls. Cyber Attacks. Theft and Robbery	Firewall, policies Antivirus, Physical Security Measures	Possible	Moderate	High	3
Reputation and Public Trust	Negative publicity, unethical behavior by staff or board members, Lack of Accountability	Clear Communication(internal and external), Form strategic partnerships	Possible	Moderate	High	4
Volunteers , workers and Human Resources	Misuse of Donor Information. Lack of Confidentiality. Misuse of Funds, Coworkers hijacking	Regular Backups, Log in sessions, Authentication mechanisms, Workers and volunteers training.	Possible	Minor	Medium	5

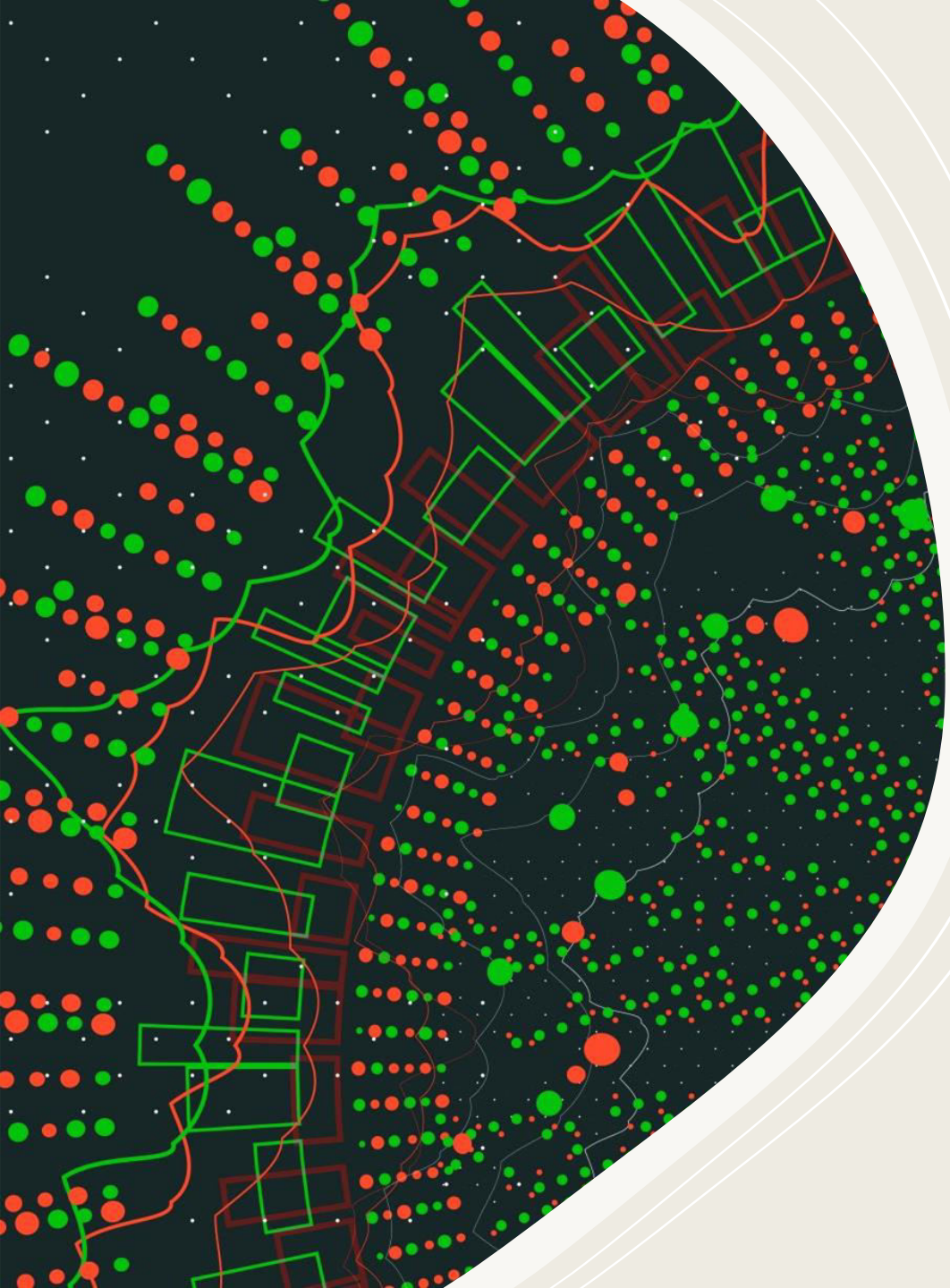

Backup and Encrypt Data
Authentication and Access Controls
An incident Response Plan and firewall
Awareness and training of the employees
Baseline controls

Implementation plan

Some risks can be accepted/avoided because the damage is tolerable and its not so common to happen; like

Coworkers hijacking , Misuse of Funds or Donor Information
the company already have log in sessions , trains its workers and some ethical policies no need to add more controls

ASSET	RECOMMENDED CONTROLS	SELECTED CONTROLS
Donor and Member information.	1- Establish strong access controls 2- Implement role-based access controls (RBAC) 3- Implement email filters and anti-phishing 4- Regularly monitor and audit systems for unusual activity	1 , 2 , 3 and 4
Information Technology Systems and Data.	1-Enforce a strong password policy and Implement multi-factor authentication 2- Regularly backup critical data 3-Conduct regular vulnerability assessments and penetration testing to identify weaknesses.	1 , 2 and 3
Finance wise assets.	1-Establish policies and procedures for handling financial transactions 2-intrusion detection systems (IDS), and intrusion prevention systems (IPS) in addition to the FW 3-Implement physical security measures(cameras, and alarm systems)	1 , 2 and 3
Reputation assets.	1-Monitor social media channels and online platforms 2-Establish ethical standards 3-Regularly review and update organizational policies 4-Implement strong governance structures and clearly defined roles and responsibilities for staff and volunteers.	1 , 3 and 4
Volunteers , workers and Human Resources.	1-Implement strong data protection to safeguard donor information prevent unauthorized access or misuse 2-Restrict access to confidential information 3-Implement strong internal controls over financial transactions 4-Foster a positive and respectful work environment to minimize the likelihood of coworker conflicts or malicious actions.	1 , 2 , 3 and 4



Giving joy socials:

Giving.joyy

Giving Joy Foundation