Access Risk Management Implementation Plan.

- **Create a list of Cybersecurity Implementation controls discussed in class for**

- Identification Credentials
    - ID Card – It is used to prove the identity of the person.
    - Photograph – It is used in identification of individual.
    - Password – It is a secret word or expression used by authorized persons to prove their right to access, information, etc.
    - Digital Signature – It is an electronic signature which can be used to provide added assurance of evidence of origin, identity, and status of an electronic document.
    - PINs – It is used in the process of authenticating a user accessing a system.
    - PKI Certificates – It is a Secure Socket Layer (SSL) certificate that uses public-key infrastructure for encryption and authentication.
    - Biometric reference samples – is data obtained by a biometric system's capture device - such as a facial image, voice recording or a fingerprint.

- Personal Authentication
    - Password – It is a secret word or expression used by authorized persons to prove their right to access, information, etc.
    - Smart Card – It is a physical electronic authorization device, used to control access to a resource.
    - Biometric reference samples – is data obtained by a biometric system's capture device - such as a facial image, voice recording or a fingerprint.
    - Access control lists – It is a list of permissions attached to an object and specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.
    - Policies – It is a deliberate system of principles to guide decisions and achieve rational outcomes.
    - Privilege token database – It is a list of users with permissions to specific resources.

- Authorization:
    - Access control lists – It is a list of permissions attached to an object and specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.
    - Security Token – A security token is a physical device used to gain access to an electronically restricted resource. The token is used in addition to or in place of a password.
    - Deny by default policy - Deny by default is a ruleset for a firewall or router that denies all incoming and outgoing traffic that is not expressly permitted.

- Logical Access Control Methods:
    - Network Architecture Controls – It is a suite of network protocols for control of entertainment technology equipment, particularly as used in live performance or large-scale installations.
    - Remote Network Access – It is a combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.
    - Securing Network Ports – Only a few important ports use by the organization must be open.
    - Physical security for Secure Internet Protocol Router Network (SIPRNet) Ports – Transmit sensitive information by packet switching over the 'completely secure' environment.
    - Logical Network Port Security – logical ports created in that network will inherit the port security value from the network.
    - Port authentication using 802.1x – It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
    - Network access control systems – It an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.
    - Password – It is a secret word or expression used by authorized persons to prove their right to access, information, etc.
    - PINs – It is used in the process of authenticating a user accessing a system.
    - Encryption – process of converting information or data into a code, especially to prevent unauthorized access.
    - PKI Compliance Requirements – A list of some of the components of Entrust products and the standards with which these products comply.
    - DoD Common Access card – It is the standard identification for Active-Duty United States Defense personnel.
    - Alternative login token – It used by NIH system administrators (Secondary account holders) for privileged access to NIH computers and information systems; it does not open gates or doors.

- Physical Access Control Methods
    - Defense Biometric Identification System (DBIDS) – It is an integrated Identity Management and Force Protection system developed and operated by the Department of Defense.
    - Badges – Used as an ID for identification of personnel.
    - Smart cards – It is a physical electronic authorization device, used to control access to a resource
    - Physical Tokens – It is a physical device used to gain access to an electronically restricted resource. The token is used in addition to or in place of a password.

    - Physical Intrusion Detection Systems – These include alarms, video surveillance, security guards etc.

- Biometric Systems
    - Fingerprint Scanner – It is a security device that uses a scanned image of your fingerprint to authenticate who you are.
    - Face Detection – It is used in a variety of applications that identifies human faces in digital images.

➢ **Create a list of Cybersecurity Implementation controls that exist at your company**

- Identification Credentials
    - ID Card – In the organization, ID cards are the primary form of identification.
    - Photograph – Photograph is present in the ID card which acts as a primary proof of identity.
    - Password – All the employees have their own passwords and its company policy that the passwords should be changed every 30 days. Also, a password must contain an uppercase, a lowercase and a numeric. Additionally, last 3 previously used passwords cannot be used again.
    - Digital Signature – It is an electronic signature which can be used to provide added assurance of evidence of origin, identity, and status of an electronic document. They are used when confidential or sensitive information is involved.
    - PINs – All employees have their own PIN's for authentication.
    - PKI Certificates – PKI Certificates are used in the company for securing emails and smart card authentication.

- Personal Authentication
    - Password – All the employees have their own passwords and its company policy that the passwords should be changed every 30 days. Also, a password must contain an uppercase, a lowercase and a numeric. Additionally, last 3 previously used passwords cannot be used again.
    - Access control lists – It is a list of permissions attached to an object and specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.
    - Policies – There are many policies, procedures, standards, and guidelines existing in the company like the employee conduct policies, HR policies etc.

- Authorization:
    - Access control lists – It is a list of permissions attached to an object and specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

    - Security Token – RSA tokens are used by the employees to gain access to an electronically restricted resource.

- Logical Access Control Methods:
    - Network Architecture Controls – It is a suite of network protocols for control of entertainment technology equipment, particularly as used in live performance or large-scale installations.
    - Remote Network Access –Employees can connect via VPN and have access to company resources.
    - Securing Network Ports – Only a few important ports used by the organization must be open. They are set in the form of firewall policies.
    - Port authentication using 802.1x – It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
    - Network access control systems – They use endpoint security to control access to an organization's network. Other devices do not connect to the network unless explicitly stated by company policy.
    - Password – All the employees have their own passwords and its company policy that the passwords should be changed every 30 days. Also, a password must contain an uppercase, a lowercase and a numeric. Additionally, last 3 previously used passwords cannot be used again.
    - PINs – All employees have their own PIN's for authentication.
    - Encryption – Data is the most important asset at our organization. Hence, data is not only encrypted at rest and in motion but also while its being processed by applications and databases.
    - PKI Compliance Requirements – A list of some of the components of Entrust products and the standards with which these products comply.
    - DoD Common Access card – It is used only while working with government clients.

- Physical Access Control Methods
    - Badges – Used as an ID for identification of personnel.
    - Physical Tokens – Physical Tokens provided by RSA security are used to access restricted electronic resources. Apart from physical tokens, virtual tokens on phones can also be used.
    - Physical Intrusion Detection Systems – Our organization include alarms, video surveillance, and security guards.

- Compare the Implementation controls discussed in class with your company's existing Cybersecurity Implementation controls

Implementation Controls	Status
Identification Credentials	
ID Card	Fully Implemented
Photograph	Fully Implemented
Password	Fully Implemented
Digital Signatures	Partially Implemented
PIN's	Fully Implemented
PKI Certificate	Fully Implemented
Biometric reference samples	NOT Implemented
Personal Authentication	
Password	Fully Implemented
Smart Card	Partially Implemented
Biometric reference Sample	NOT Implemented
Access control lists	Fully Implemented
Policies	Fully Implemented
Privilege token database	NOT Implemented
Authorization	
Access control lists	Fully Implemented
Security tokens	Fully Implemented
Deny by default policy	NOT Implemented
Logical Access Control methods	
Network Architecture controls	Fully Implemented
Remote Network Access	Fully Implemented
Security Network ports	Fully Implemented
Physical Security for Secure Internet Protocol Router Network (SIPRNet) Ports	NOT Implemented
Logical Network Port Security	NOT Implemented
Port Authentication using 802.1x	Fully Implemented
Network Access Control systems	Fully Implemented
Passwords	Fully Implemented
PIN's	Fully Implemented
Encryption	Fully Implemented
PKI Compliance Requirements	Fully Implemented
DoD Common Access Card	Partially Implemented
Alternative login token	NOT Implemented
Physical Access Control Methods	
Defense Biometric Identification System (DBIDS)	NOT Implemented
Badges	Fully Implemented
Smart cards	Partially Implemented
Physical Tokens	Fully Implemented

Physical Intrusion Detection Systems	Fully Implemented
Biometric Systems	
Fingerprint Scanner	NOT Implemented
Face Detection	NOT Implemented

- **Create a list of critical assets in $ that exist in your company**

Data is the most important asset at our company

Some of the critical assets are:

Patients health records: Maintaining Patients health records is crucial to our organization. It will cost millions if there is any breach involving patient's health records.

Client Information: Doctors and patient's information are one of the crucial assets. Damage control will cost millions if there are any data leaks.

Employee Information: It consists of HR records. Damage control and credit monitoring services would cost the company thousands of dollars of there is a breach.

Organization Reputation: Positive Reputation for a corporation is essential for building trust and is one of the critical asset. It is intangible.

- Create a list of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing
    - Loss of Authentication
    - Unauthorized Access
    - Unauthorized modification
    - Vulnerabilities related to network related attacks

- Create a list of potential threats to your company that could exploit vulnerabilities of critical assets.
    - Network Related Attacks
    - Loss of Reputation
    - Disclosure of sensitive information

- Create a list of potential risks for critical assets where Cybersecurity Implementation Controls are missing
    - Unauthorized access
    - Disclosure of sensitive information
    - Loss of integrity

- **Provide a list of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks (it is not required to write detailed policies) – Risk Prevention Strategy.**

    - Biometric systems need to be implemented for improved authentication. They provide improved security and cannot be forgotten or lost.
    - Implementing a deny by default policy on the company firewall provides us with a better control over authorization. All the ingress traffic from the internet is denied by default.
    - Logical Network Port Security should be implemented so that all the unnecessary ports can be closed and be less susceptible to attacks from the internet.
    - Data loss prevention software should be implemented to protect all the sensitive information and to tighten endpoint security

- **Provide a list of recommended Hardening methods and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience (it is not required to write detailed policies) – Risk Response Strategy.**

    - Data Activity Monitoring (DAM) solution can be implemented to closely monitor traffic and to avoid data leaks. An average hacker conducts reconnaissance six months before the actual breach, hence monitoring for unusual behavior can help deter a data breach.
    - A Host based Intrusion Detection System and Network based Intrusion Detection System can be implemented for closely monitoring, analyzing the packets, logging, and notifying authorities.
    - Full scans must be run for malware from time-to-time basis.

- **Create a detailed policy for the Remote Access control using a SANS template as provided in class**

Remote Access Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

The purpose of this policy is to define standards for connecting to company's network from any host. These standards are designed to minimize the potential exposure to company from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical company internal systems, etc.

2.0 Scope

This policy applies to all company employees, contractors, vendors, and agents with a company-owned or personally owned computer or workstation used to connect to the company network. This policy applies to remote access connections used to do work on behalf of company, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of company employees, contractors, vendors, and agents with remote access privileges to company's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to company.

2. General access to the Internet for recreational use by immediate household members through the company Network on personal computers is permitted for employees that have flat-rate services. The company employee is responsible to ensure the family member does not violate any company policies, does not perform illegal activities, and does not use the access for outside business interests. The company employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of company's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*
4. For additional information regarding company's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases. For information on creating a strong passphrase see the Password Policy.
2. At no time should any company employee provide their login or email password to anyone, not even family members.
3. company employees and contractors with remote access privileges must ensure that their company-owned or personal computer or workstation, which is remotely connected to company's corporate network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.
4. company employees and contractors with remote access privileges to company's corporate network must not use non-company email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct company business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the company network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
9. All hosts that are connected to company internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to

corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third-Party Agreement*.

10. Personal equipment that is used to connect to company's networks must meet the requirements of company-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the company production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Cable Modem over Cable	Cable companies such as AT&T Broadband provide Internet access

TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus, the name "modem" for modulator/demodulator.

Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or another Internet service provider (ISP). Being on a company-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into company and an ISP, depending on packet destination.

DSL Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay A method of communication that incrementally can go from the speed of an

ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage.

Frame Relay connects via the telephone company's network.

ISDN There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access Any access to company's corporate network through a non-company-controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-company network (such as the

Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into company's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Version	Revision Date	Author
1.0	**10/20/2019**	**Abhishek Ningala**