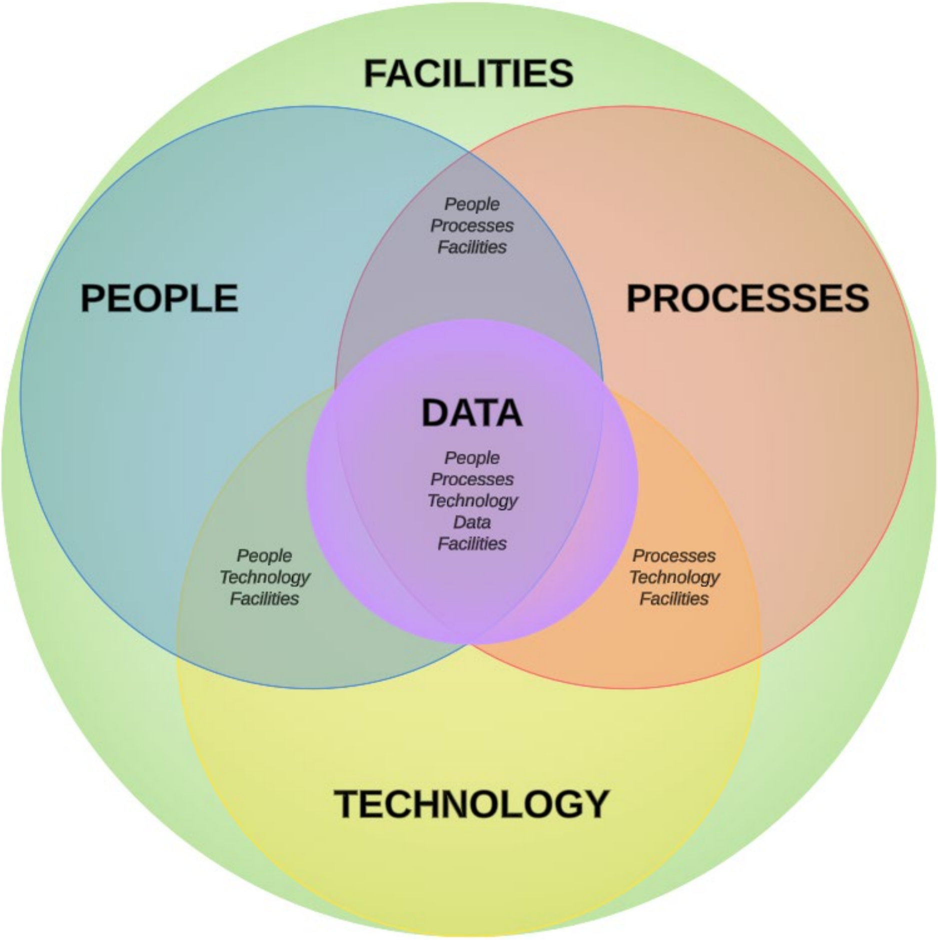
People, Processes, Technology, Data & Facilities (PPTDF)
Control Applicability Model

The People, Processes, Technology, Data & Facilities (PPTDF) model shows that a multi-faceted approach to control applicability is indispensable, where it can create a resilient defense against a myriad of physical and cyber threats. A proactive stance in implementing and refining these controls will be crucial in securing the ever-expanding digital frontier.



These examples help demonstrate the applicable nature of controls:

- You cannot apply end user training to a firewall (technology).
- An employee (people) cannot have a secure baseline configuration applied.
- An Incident Response Plan (IRP) (process) cannot sign a NDA, use MFA or be patched.
- Controlled Unclassified Information (CUI) (data) cannot be assigned roles and responsibilities.
- Your data center (facility) cannot undergo employee background screening.

The PPTDF model, encompassing People, Processes, Technology, Data, and Facilities, provides a comprehensive approach to cybersecurity control applicability, as described below:

People
People are often considered the weakest link in cybersecurity. Human error, negligence, or malicious intent can lead to significant vulnerabilities. To mitigate these risks, organizations implement human-specific controls such as:

Security Awareness Training: Educating employees about cybersecurity best practices and potential threats.
Access Controls: Enforcing the principle of least privilege to restrict access based on job roles.
User Authentication and Authorization: Implementing strong authentication mechanisms and carefully managing user permissions.

Processes

Effective cybersecurity processes are essential for identifying, responding to, and mitigating threats. Common processes that exist as controls include:

- Incident Response Plans: Establishing well-defined processes to respond promptly and effectively to security incidents.
- Regular Audits and Assessments: Conducting periodic assessments to identify vulnerabilities and measure compliance with security policies.
- Change Management: Implementing controls to manage changes in technology and processes to avoid unintended security consequences.

Technology

The technological aspect of cybersecurity involves deploying and configuring tools to protect against threats. Common technologies that exist as controls include:

- Network Defenses: Filtering and monitoring network traffic to prevent unauthorized access (e.g., firewalls, Intrusion Protection Systems (IPS), Data Loss Prevention (DLP), etc.).
- Endpoint Protection: Installing antimalware software, Endpoint Detection and Response (EDR) tools to secure individual devices, etc.
- Encryption: Safeguarding data in transit and at rest through robust encryption mechanisms.

Data

Data is at the heart of the PPTDF model, making data protection truly the central focus of cybersecurity controls. There are many types of data that are considered sensitive/regulated that include, but are not limited to:

- Controlled Unclassified Information (CUI),
- Federal Contract Information (FCI),
- Personally Identifiable Information (PII),
- Cardholder Data (CHD),
- Export-Controlled Data (ITAR / EAR),
- Electronic Protected Health Information (ePHI),
- Intellectual Property (IP),
- Critical Infrastructure Information (CII),
- Attorney-Client Privilege Information (ACPI) and
- Student Educational Records (FERPA).

These data types have specific controls that are dictated by applicable laws, regulations or contractual obligations and include:

- Data Classification: Data must be categorized to apply the appropriate security measures.
- Limited Access: Data must be protected by limiting logical and physical access to data to individuals and systems that have a legitimate business need.
- Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) Data: Data must be trustworthy, based on the data's currency, accuracy, integrity and/or applicability.
- Availability: Data must be available, which involves regularly backing up data and establishing effective data recovery mechanisms that protects the integrity and confidentiality of the data being backed up and recovered.

Facilities

Physical security is often overlooked but plays a crucial role in overall cybersecurity and data protection. Common physical controls include:

- Physical Access Control (PAC): Restricting physical access to any facility where systems or data exist. PAC exists in more than datacenters and corporate offices. The concept of PAC extends to home offices and Work From Anywhere (WFA) workers who still have an obligation to apply physical security protections to their systems and data.
- Surveillance Systems: Monitoring and recording activities within facilities to detect and deter unauthorized access.
- Environmental Controls: Maintaining optimal conditions for hardware to prevent damage or disruptions.