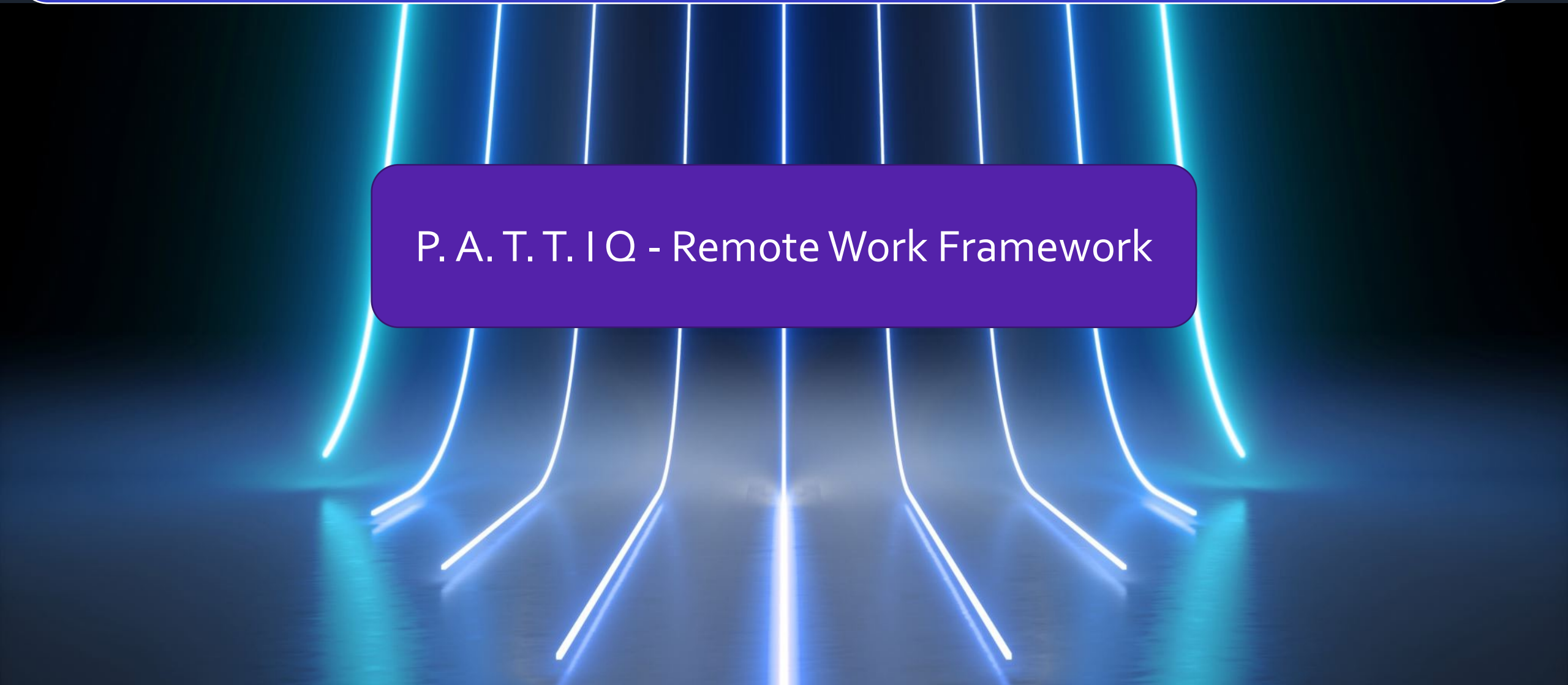
# JCJ Alliance



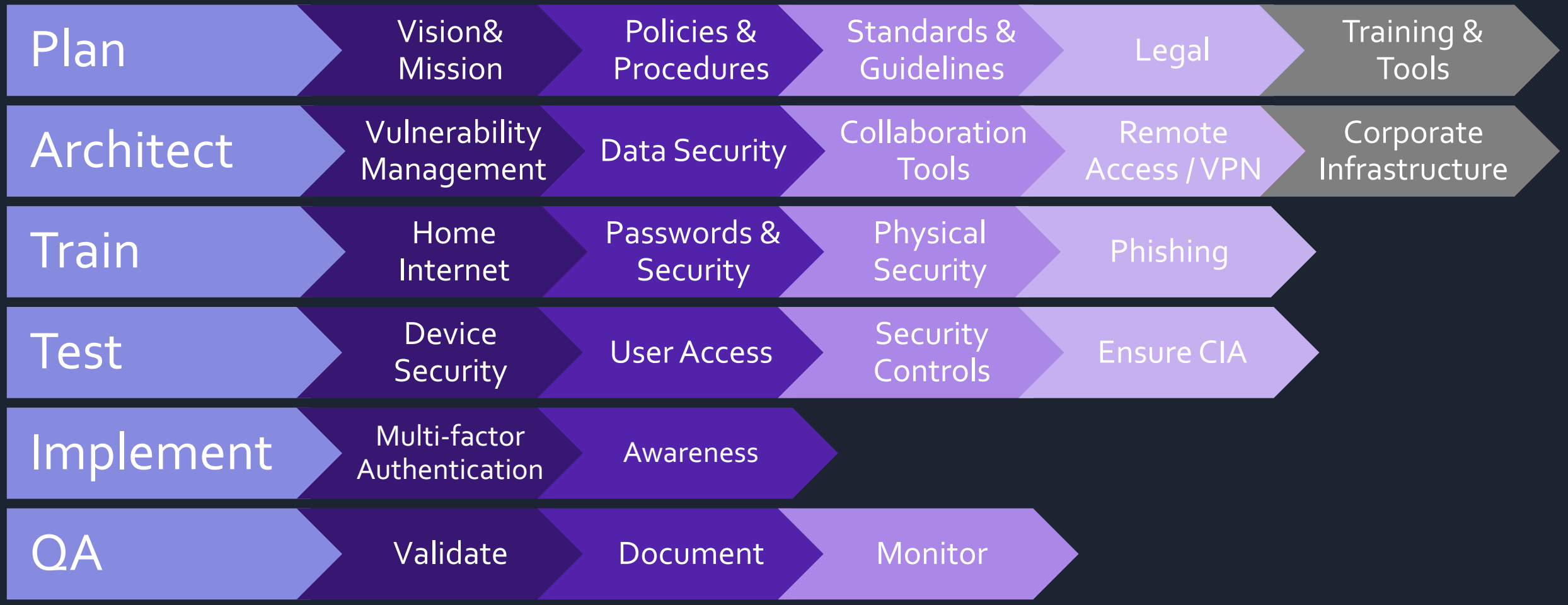
## P. A. T. T. I Q - Remote Work Framework

# Executive Summary

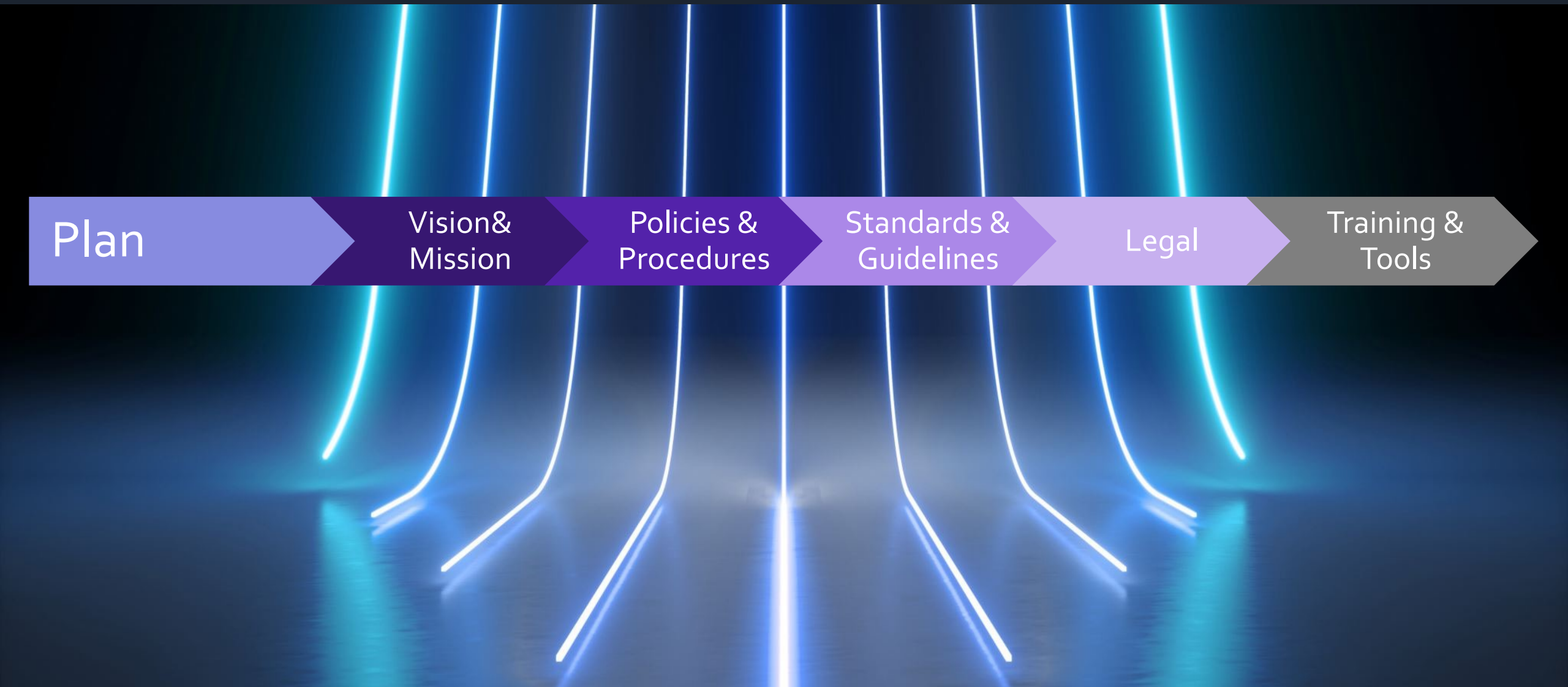
JCJ Alliance is a group of cybersecurity professionals who have created this open-source framework to streamline the process of converting your On-Premises employees to Work-from-Home employees. We understand how this may present a challenge to organizations that may lack the policies, technology, and training to secure a remote workforce. We also understand, from experience, how employees may be unfamiliar or uncomfortable with the idea of working from home. The purpose of this framework is to provide security concepts to be discussed by your company's Information Security and Information Technology teams. We recommend you focus just on the most important concepts that will have the greatest impact on your organization and implement the processes that will help maintain your company's Confidentiality, Integrity, and Availability while your employees are working off-site.

We have designed these concepts with a focus on the financial industry, but we believe this framework can easily be adopted by Cyber Security professionals across all industries. We hope this strategic framework helps to address your most pressing security concerns related to creating a work-from-home workforce and makes your conversion process as simple as possible.

# P. A. T. T. I Q – Remote Work Framework



# P. A. T. T. I Q – Remote Work Framework



# Vision & Mission

Reimaging your vision and mission

As a good builder, you need to start from the foundations; the company's vision and mission. Now that remote work is the norm, your employer branding will benefit from a tweak. You can brush it up and reconstruct it by prioritizing the new values you'd like to embrace. Flexibility, adaptability, and agility are some of them.

# Policies & Procedures

Create a policy that is tailored to the needs of remote employees. Not all jobs should be done outside of the office. Any position that works from home will benefit from the policies and procedures you develop.

# Standards & Guidelines

Set goals to make sure your remote workers have the tools they need to carry out.

Be sure that all remote employees have access to the systems, programs, and tools that are normally used to perform their duties.

Evaluate if sufficient protection and data privacy are in effect when accessing, sending, receiving material, and including paper copies of records they may have at home.

Remote workers should create a comfortable, functional workspace, that minimizes at home distractions.

Create a system for tracking and approving hours. If handling non-exempt workers, be sure they let management know when they’re going to take a break.

# Legal

Clearly outline the legal rights that remote workers have.

Remote workers are entitled to the same legal protections that in-office workers have. However, working remotely can present some added challenges that need to be addressed to ensure your company is legally compliant.

Set up a process to report hours for hourly remote workers.

It's important to support employees that are remote just as you would in-office workers.

# Training & Tools

Provide the right tools for successful and secure work.

Your employees need the right tools to work securely and productively.

Additionally, cybersecurity concerns should be top-of-mind. Remote workers might need a VPN or another form of security to work on important company files or private customer data. And while some employees might be able to operate using public Wi-Fi networks, others might need to stay at home or in a more secure co-working space to ensure data privacy.

You'll also need policies and tools in place for remote team collaboration and communication.

# P. A. T. T. I Q – Remote Work Framework

# Vulnerability Management

Vulnerability Management is necessary whether your organization allows remote work or solely works from the office. There are several frameworks that cover Patch and Vulnerability Management. At its core vulnerability management is used to keep systems up-to-date and reduce the risk of computing resources. Two of the most recognized and followed are from SANS and NIST.

# Data Security

As with many other aspects, securing corporate data is extremely important whether you have employees working remotely or not. Ensuring security of your data relies with proper access restrictions and encryption. Data should be encrypted both in-transit and at rest

# Collaboration

Make sure that you have chosen which tools are acceptable for collaborating. Many users already have Zoom or other collaboration tools installed. To ensure security of your data, you will want to leverage corporate approved solutions whether its Zoom, WebEX, GoTo Meeting or another tool.

# Remote Access

There are many solutions available for remote access. You may already have a remote access or VPN connectivity available for your staff. Directing users to login to a Virtual Desktop environment (such as Citrix VDI, VMware Horizon, or Microsoft VDI) can greatly increase your ability to maintain data security since these solutions allow users to connect to a device that is within your infrastructure already adheres to you patch management and security policies.

# Corporate Infrastructure

When considering a remote work strategy additional infrastructure may be required. At a high level you will need to consider the following factors:

- Compute Resources
- Software Licensing
- Network Bandwidth
- End user device strategy

# P. A. T. T. I Q – Remote Work Framework

# Home Internet

Researchers at San Francisco State University recommend internet speeds above 5 Mbps as speeds below 5 Mbps are not adequate for two-way interaction on Zoom. For glitch-free video meetings, they recommend at least 20 Mbps download and 3 Mbps upload speeds.

The best internet speed for working from home depends on the user's job function. If a user frequently downloads and uploads large files and participates in video meetings, ideally at least 25 Mbps is recommended. Conversely, if the user will not be downloading large files or participating in Zoom meetings lower Mbps should suffice.

# Passwords & Authentication

Passwords alone are no longer a sufficient means to protect our valued information. Weak passwords continue to be one of the primary drivers for breaches on a global scale.

Educate your staff on the four key behaviors that can help mitigate brute force or password cracking attempts.

Multi-factor authentication (MFA), also referred to as two-factor authentication, help prevent unauthorized access to the protected account if your credentials become compromised.

Enabling MFA reduces account compromise by 99 %

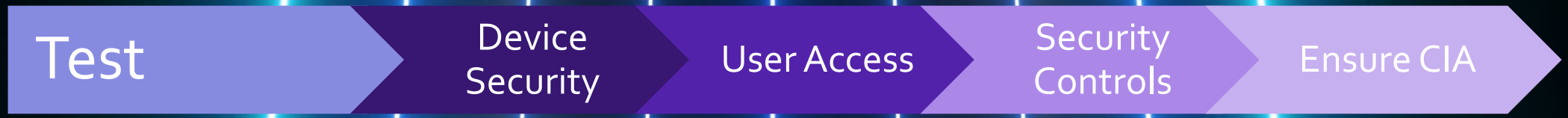
# Physical Security

Physical security for your business should remain a priority while you are off-site. Consider utilizing remote security technology like, Intrusion Systems, Access Control Systems, and Video Surveillance Systems to help secure your facility and maintain the health of your systems without ever stepping foot on-site.

# Phishing

One of the greatest risks remote workers will face is social engineering attacks. Social Engineering is a psychological attack where attackers trick or fool their victims into making a mistake, which will be made easier during a time of change and confusion. The key is training people on what social engineering is, how to spot the most common indicators of a social engineering attack, and what to do when they spot one. Be sure you do not focus on just email phishing attacks, but other methods to include phone calls, texting, social media or fake news.

# P. A. T. T. I Q – Remote Work Framework



# Device Security

It is necessary for all those who are working from home to take some of the security measures to safeguard their confidential data. It is one thing for a personal Instagram account to be hacked. But leaking your employer's sensitive data due to an unsecure network? That is a much more serious problem for your company. Taking steps like encrypting your Wi-Fi signal, updating your router's firmware, and using a VPN (virtual private network) are essential to keeping your work life secure.

- Below are a few tips that could be helpful for IT professionals and your staff.
- If you need to leave your home for supplies or other reasons, make sure your work devices are either shut down or locked — including any mobile phones you might use to check email or make work phone calls.
- If you live with a roommate or young children, be sure to lock your computer even when you step away for just a bit. Do not tempt your roommates or family members by leaving your work open. This is true even for the workplace, so it is imperative for WFH.
- If you cannot carve out a separate workspace in your home, be sure to collect your devices at the end of your workday and store them someplace out of sight. This will not only keep them from being accidentally opened or stolen but will also help to separate your work life from your home life.

# User Access

Confirm users can access the remote resources.
Engage one user from each team to perform a “pretend it's real” run though. Provide a checklist of services and applications the user will need to validate.

# Security Controls

Employing only one of the following security measures will not be enough to thwart cyber threats. Each security measure, in isolation, will not guarantee secure remote work; however, when used in tandem with multiple measures, it creates a compounding effect for your cybersecurity. Consider implementing the following security controls to ensure Defense in Depth:

**Separate work and personal devices**

- **Use encrypted communication service**
- **Employ the Principle of Least Privilege**
- **Remove Orphaned Accounts**

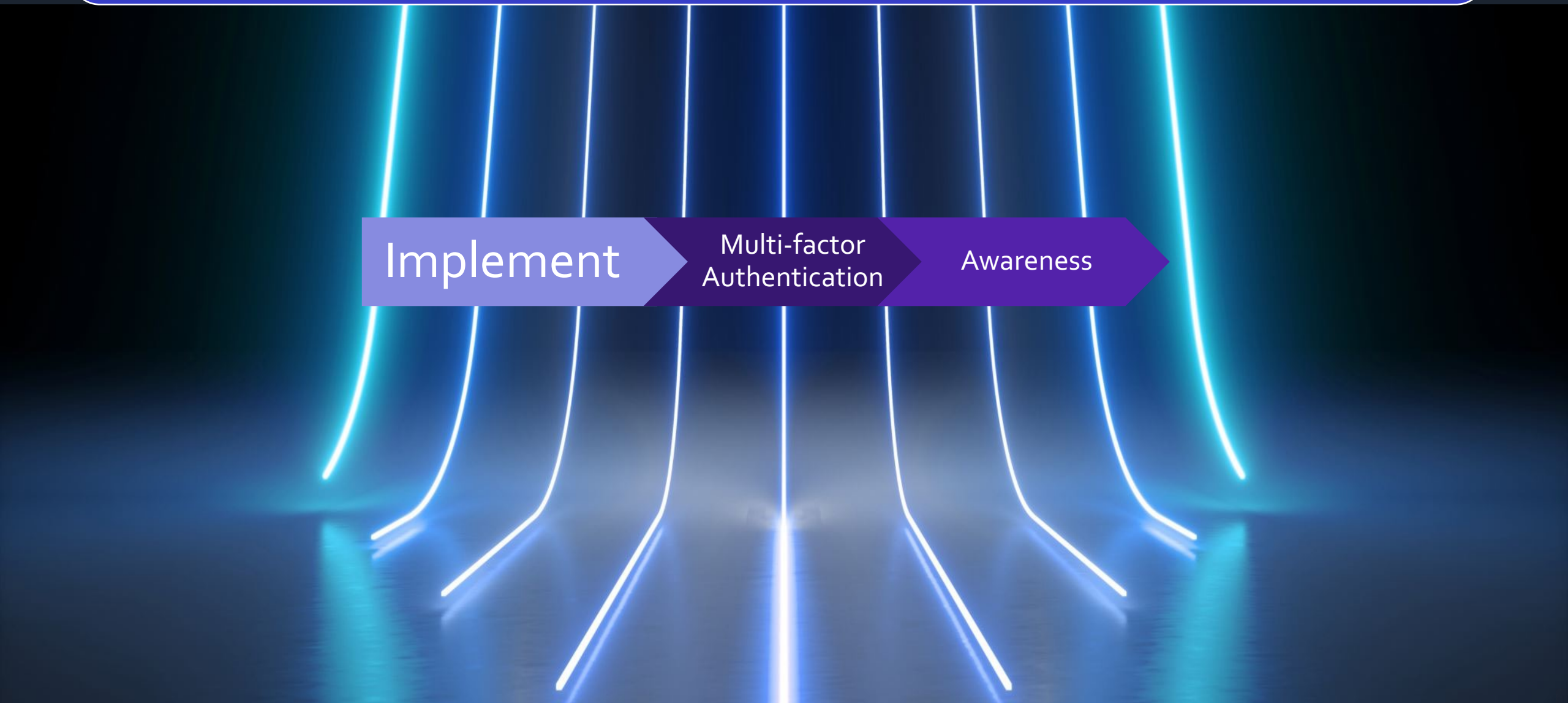
# Ensure CIA

It is essential to maintain Confidentiality, Integrity, and Availability while working from home.

Utilize a VPN that uses proper encryption over the end-to-end connection.

- Instead of only utilizing standard authentication with either a pre-shared key (bad idea) or username and passwords that can be compromised through brute force attacks, implement multi-factor authentication (MFA).
- Once connected to the corporate network, utilize the least privileged access.
- Increase the log monitoring activities and look for abnormal behavior.
- Change the way you perform threat analysis.
- Before systems connect, ensure you have policies implemented that all systems shall be up to date with their patches and anti-malware definitions.

# P. A. T. T. I Q – Remote Work Framework



# Multi-Factor Authentication (MFA)

Implementing Multi-Factor Authentication (or "MFA") can greatly reduce account compromise. If a user's password is stolen it is of no value without an additional factor. There are many vendors offering MFA solutions. You may find that you will need more than one to cover all resources since some applications or vendors may only allow use of specific token provider.

What is MFA anyway? MFA refers to entering a username along more than one "factor" to gain access. The main factors are:

- Something you know (examples: A password or PIN)
- Something you have (examples: A smartcard, a security token)
- Something you are (examples: A fingerprint, your iris, your voice)

# Awareness

Security is everyone's job. When companies shift how personnel are allowed to connect to corporate resources, they must also keep in mind how those changes impact your security posture. This is where the training program comes into play. Users must be aware of different factors when working remotely. If at home, they should keep in mind their WiFi security. Whereas in the office or connecting from another location they should be aware of who may be around that can view their screen or might have access to their personal belongings.

# P. A. T. T. I Q – Remote Work Framework

# Validate

Once you have staff working from home you will need to verify that the user experience essentially mimics being in the office. In some cases, this could mean having to hardwire devices to you users' home router. Other situations could require upgrading internet service.

# Document

Documentation is an important and often overlooked step. Confirm that all documentation is complete prior to closing out the project. This should include everything from the Statement of Work, to Policies & Procedures, Standards & Guidelines, Training materials, detailed architectural documents, and issues with steps taken to resolve.

IT architecture diagrams should include network diagrams with IP addresses, ports, applications, services, and accounts.

All documentation should be reviewed during the QA phase to confirm that changes during the implementation are accurately reflected.

# Monitor

Network logs should be reviewed to confirm that any new vulnerabilities are being blocked and new, legitimate, traffic is being allowed.