Business Continuity Risk Readiness

Strategy and Self-Assessment tool

In the current COVID-19 pandemic, the global urgency for businesses, governments, families, and individuals to be able to work from home is unprecedented. This document can help you navigate these profound challenges. Basic questions you may be facing are, "Where do I begin?" or "What can I do right now while keeping safety a top focus?"

The COVID-19 pandemic has forced organizations to review their Digital Transformation Plans and, in particular, the Work from Home Business Continuity Plan (BCP/WFH). In this process, infrastructure capacity and remote access functionalities are top priority. Sending home an entire corporation's workforce requires immediate analysis of the infrastructure capacity for remote access service. Less obvious, however, is that the organization's business risks will increase with the expansion of the corporation attack surface, extended by multiple remote workers.

This assessment offers the first step in actively keeping your business running securely while keeping employees and customers safe. Through a series of discovery questions, IT and security roles can determine the current state of your organization and how you can achieve full functioning by incorporating best practices identified by Cisco® Trusted experts.

Remote access affects two main corporate user groups: contractors, working on site or remote, and regular employees working typically on site and eventually remotely. The first group generally have a well-defined limited access, framed by their service contract and imposed by rigorous IT security policies and infrastructure. The corporate employee group works mainly from the office, where a less restrictive security policy is often allowed. Employee remote access is thus limited in infrastructure and time usage, which is perceived as "limited" or "controlled" risk. The Work from Home Business Continuity Plan remains a business risk mitigation measure, and the Security Team should take part in the plan review exercise.

As you discover your level of readiness and where your areas of risk are, you can identify what you can do first, and learn how to improve your readiness for the future. Cisco IT offers best practices across processes and technologies for business continuity to enable remote work with effective, secure, and collaborative solutions.

As we transition to the next phases of the pandemic, your business is being redefined by the changes of today and the uncertainties of tomorrow. These factors have accelerated the digital transformation trends that were already in motion. Cisco provides ways to connect your people, secure your business and automate processes in the evolving distributed work-model with a set of offerings to help you re-imagine and redesign your workforce and workplaces.

Solutions When It Matters Most: Work from Home Readiness and Business Continuity Strategy

Vision
Remote Workforce Requirement for Effective Business Continuity

Effective change starts by establishing a clear and **Realistic Vision** aligned with the company business goals

Motivation
COVID-19, Employee Health, Legal Requirements

In the current environment external forces drive your Organization's **Incentive for Change**

Resources
Employees, Contractors, Partners, Customers, Infrastructure

Comprehensive change plan that will affect the entire **Organization Ecosystem**

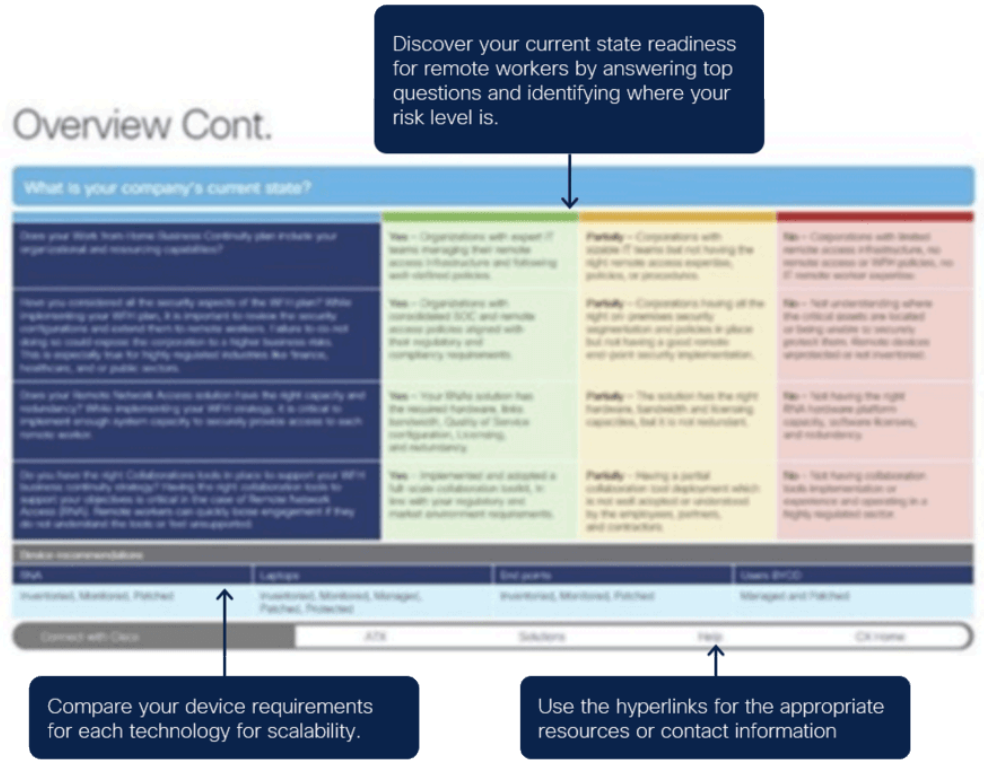
Action Plan
Organization, Security, Remote VPN, Collaboration tools

Action plans based on Best Practices and expert guidance, will lead to **Predictable Outcomes**

In the dynamic situation created by COVID-19, use this Remote Worker Experience and Strategy assessment to help you navigate the current unprecedented challenges, technology options, and business process strategies now available.

How to Use This Assessment

Use this high-level assessment for a quick overview of glance into your organization's current state, identify where the technical gaps are, and view Cisco recommendations and delivery capabilities.



Overview

Your Corporate Business Continuity Plan includes multiple aspects beyond simply the IT domain. These various dimensions are even more important as your organization is in the middle of a digital transformation. When planning for Work from Home Business Continuity, four aspects are essential to review: organizational readiness, approach to security, remote access infrastructure, and collaboration solutions.

Good Practices

- **Prepare Your Organization for Change:** Successful change requires properly communicating the vision and action plan, plus having the right skills, motivation, and resources
- **Review** your IT organization readiness
- **Review** your processes, policies, and compliance readiness regarding remote workers
- **Review** critical assets and endpoints protection readiness
- **Review** your remote access capacity and redundancy

Outcomes

- Increased productivity
- Managed cost control
- Effective employee retention and engagement

Capabilities


Organization


Collaboration


Security


Remote Network Access

Overview Cont.

What is your company's current state?

Does your Work from Home Business Continuity plan include your organizational and resourcing capabilities?	**Yes** – Organizations with expert IT teams managing their remote access infrastructure and following well-defined policies.	**Partially** – Corporations with sizable IT teams but not having the right remote access expertise, policies, or procedures.	**No** – Corporations with limited remote access infrastructure, no remote access or WFH policies, no IT remote worker expertise.
Have you considered all the security aspects of the WFH plan? While implementing your WFH plan, it is important to review the security configurations and extend them to remote workers. Failure to do not doing so could expose the corporation to a higher business risks. This is especially true for highly regulated industries like finance, healthcare, and or public sectors.	**Yes** – Organizations with consolidated SOC and remote access policies aligned with their regulatory and compliancy requirements.	**Partially** – Corporations having all the right on-premises security segmentation and policies in place but not having a good remote end-point security implementation.	**No** – Not understanding where the critical assets are located or being unable to securely protect them. Remote devices unprotected or not inventoried.
Does your Remote Network Access solution have the right capacity and redundancy? While implementing your WFH strategy, it is critical to implement enough system capacity to securely provide access to each remote worker.	**Yes** – Your RNAs solution has the required hardware, links bandwidth, Quality of Service configuration, Licensing, and redundancy.	**Partially** – The solution has the right hardware, bandwidth and licensing capacities, but it is not redundant.	**No** – Not having the right RNA hardware platform capacity, software licenses, and redundancy.
Do you have the right Collaborations tools in place to support your WFH business continuity strategy? Having the right collaboration tools to support your objectives is critical in the case of Remote Network Access (RNA). Remote workers can quickly loose engagement if they do not understand the tools or feel unsupported.	**Yes** – Implemented and adopted a full-scale collaboration toolkit, In line with your regulatory and market environment requirements.	**Partially** – Having a partial collaboration tool deployment which is not well adopted or understood by the employees, partners, and contractors.	**No** – Not having collaboration tools implementation or experience and operating in a highly regulated sector.

Device recommendations			
RNA	Laptops	End points	Users BYOD
Inventoried, Monitored, Patched	Inventoried, Monitored, Managed, Patched, Protected	Inventoried, Monitored, Patched	Managed and Patched

Organizational Readiness

Organizational governance is a key consideration in assessing your readiness to effectively extend your targeted toolsets and capabilities to a work-from- home environment.

Good Practices

- **Define** a continuity plan for historically on-premise activities
- **Baseline** core safety guidelines for work-from-home environment (health and IP)
- **Facilitate and capture** productivity metrics independent of work location
- **Extend** corporate culture by including remote activities and data capture

Outcomes

- Extended productivity environments
- Safe and “ready” for business workplaces
- Remote worker visibility
- Connected workforce

Related offers:

- Pop up sites
- Virtual Visitation
- Secure Remote Worker
- Cisco DNA Spaces
- Webex Contact centre
- Virtual education
- Business Resiliency Strategy and Roadmap

Success Focus


Business Scaling


Talent Retention


Quality


Cultural Evolution


Productivity

Organizational Readiness Cont.

What is your company's current state?			
Can the remote worker task or responsibilities be carried out remotely?	**Yes** – All identified tasks and/or responsibilities can effectively be carried out remotely.	**Partially** – Some of the identified tasks will be affected by working remotely.	**No** – Critical tasks may be impacted by working remotely.
Are the work-from- home environments "safe" for business?	**Yes** – The identified working spaces have been certified "safe" and optimized for business.	**Partially** – The identified spaces are "safe" but not optimized for business.	**No** – The identified spaces are not safe" and not optimized for business.
Can employee task and assignment progress be tracked efficiently?	**Yes** – Full visibility into the remote workers' tasks and productivity can be monitored and tracked.	**Partially** – Some visibility into remote workers' tasks and productivity, but some elements are missing.	**No** – There is minimum to no visibility into the remote workers' tasks and productivity and several elements are missing.
Will the employee remain connected within the corporate culture?	**Yes** – Our corporate culture allows remote workers to feel connected, even with limited to no exposure to coworkers or clients.	**Partially** – A portion of our corporate culture that allows remote workers to feel connected, even with limited to no exposure to coworkers or clients.	**No** – Our corporate culture does not facilitate remote workers to feel connected, even with limited to no exposure to co-workers or clients.

Organizational Portfolio		
Unified	Extended	Diverse
Single business unit with defined span of control and success criteria	Several business units with separate span of control and success criteria	Multiple and diverse business units with varied span of control and success criteria

Security Strategy

Getting security right is all about the holistic consideration of the people, technologies, and processes that make up your business. To move forward, you must understanding inherent risks and take calculated steps to manage them.

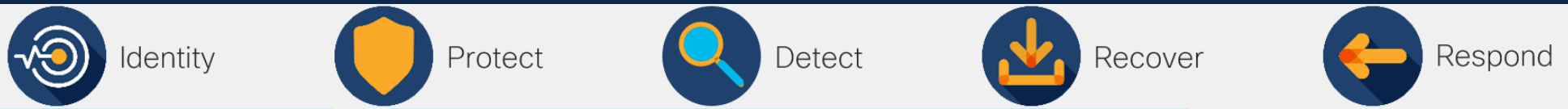
Good Practices

- **Utilize** a common security framework to cover key functions such as billing, payroll, HR, executive functions, and intellectual property
- **Maintain** policies and procedures to cover common scenarios with each function
- **Understand** the regulatory regimes under which you manage these functions
- **Assess** the risks that you're exposed to
- **Create** an action plan to treat any residual risks

Outcomes

- Ensure that the people, systems, and processes have appropriate security controls applied to protect them
- Ensure compliance when employees are working from unfamiliar surroundings
- Ensure that outstanding risks are understood and can be communicated to appropriate senior executive stakeholders

Capabilities



Security Advisory

Business Resiliency Architecture Advisory Service

Security Strategy Cont.

What is your company's current state?

Do your policies and procedures cover home working with respect to risks posed by video conferencing, file sharing, handling of personally identifiable information (PII), and malware protection?	**Yes** – Working from home is already covered.	**Partially** – Changes to out processes and policies will be necessary.	**No** – We have not actively considered working from home.
Has awareness training has been given with respect to COVID-19-related scams?	**Yes** – We regularly brief our employees on new threats and strategies that they can use to reduce their exposure.	**Partially** – We have given generic guidance.	**No** – We do not have any awareness program.
Are you considering the impact that might stem from a regulatory breach affecting PII, be that financial (PCI-DSS), privacy (GDPR) or other when you approve operational changes such as BYOD, use of cloud-based file sharing, and collaboration platforms?	**Yes** – We are not a regulated sector, or our policies and processes are deemed sufficient to cover changing employee practices.	**Partially** – We intend to review our policies and processes to ensure we remain in regulatory compliance with changing employee practices.	**No** – We have not considered the regulatory compliance impact of changing employee practices.
Have you assessed the wider impact of a work-from-home strategy on users in business-critical functions that are essential to your business?	**Yes** – We have a robust, well-tested approach and can handle any impact associated with employees working from home.	**Partially** – We're still working to address key concerns.	**No** – We do not currently have a good handle on the impact of employees working from home.

Operational Requirements		
	Small	MFA + VPN
Assessment  Engineering  Response 	Midsize	Security Framework
	Large	Framework Compliance

Connect with Cisco | ATX | Solutions | Help | CX Home

Security Operations

Operational security is all about building institutional muscle memory and making policies and processes scale with the organization. It is important to have the people and capabilities to identify, protect, detect, respond, and indeed recover the organization in the case of critical events.

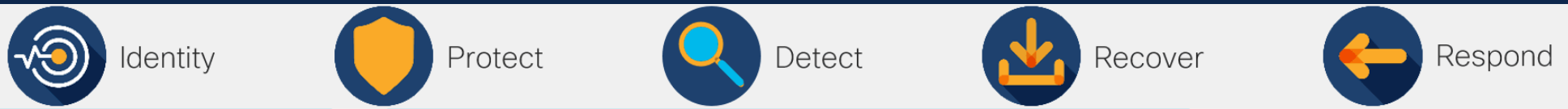
Good Practices

- **Understand** your users' and systems' "normal" behavior
- **Ensure** data is secured in transit and at rest
- **Incorporate** Multi Factor Authentication (MFA) wherever possible
- **Segment** your network to reduce potential for contagion
- **Assess** your external posture and the attack surfaces it presents regularly
- **Plan and train** for business continuity failures

Outcomes

- Ensure that the work force, work place, work flow, and work load have appropriate security controls applied to protect them
- Ensure compliance when employees are working from unfamiliar surroundings
- Ensure that new risks are understood and can be communicated to appropriate senior executive stakeholders

Capabilities



Managed Security Services

Business Resiliency Architecture Advisory Service

Security Operations Cont.

What is your company's current state?

Do you have a business continuity plan?	**Yes** – It is regularly tested.	**Partially** – But there may be gaps.	**No** – We haven't planned anything.
Have you reviewed and agreed with key stakeholders who will implement and/or be accountable for the changes that will you need to make from a security standpoint to enable home working?	**Yes** – We didn't need to change anything.	**Partially** – We've made some changes in consultation with our engineers, but we need them security tested.	**No** – We're not sure of our current asset exposure or security posture.
Are you taking active steps to secure the devices of remote workers?	**Yes** – We use MFA, VPNs, and endpoint management tools to secure employees, devices, and data.	**Partially** – Users working from home have access only to limited business services and email.	**No** – We have employees that are reliant on their own devices to access our systems.
Do you have the ability to see and respond to threats, proactively if possible irrespective of where employees and assets are located?	**Yes** – Our Security Operations Center (SOC) has the ability to monitor and support employees from any work location.	**Partially** – If there is an incident, we can call in a supplier on retainer.	**No** – We have to trust our employees not to mess with their systems.

Infrastructure Requirements		
MFA  Remote Worker Access  MDR 	Small	MFA + VPN
	Midsize	IR
	Large	MSSP

Remote Network Access (RNA)

There are multiple factors that influence any given RNA VPN solution's readiness.
It is imperative to ensure that RNA service continues to meet functional and organizational requirements. Well-designed scalable solutions provide the best experience while increasing productivity and reducing infrastructure costs.

Good Practices

- **Centralize zero-touch management** and service assurance over the Internet
- **Baseline** platform resource utilization
- **Monitor** central and remote systems resources
- **Prioritize** network traffic for critical/latency-sensitive applications. Divert local Internet traffic, by offloading "trusted" Internet traffic
- **Engineer** central clusters balancing, business requirements, costs, and cluster fail tolerance

Outcomes

- Flexible service scalability to meet business agility requirements
- Increased business agility
- Great end-user experience
- Increased workforce productivity

Increase VPN Remote Access capacity and manage security vulnerabilities with your Cisco Customer Experience team with the CX Offer for Secure Remote Workers.

If you need to expand quickly, or reconfigure your facilities to address new rules around social distancing and to keep people safe, Cisco CX can help.

CX Offer for Pop-up Sites allows you to set up a hospital, clinic, office and classroom space swiftly and securely.

CX Offer for Business Resiliency Strategy and Roadmap can help accelerate your customized strategy based on prioritized use cases.

Capabilities


Organization


Collaboration


Security


Remote Network Access

Remote Network Access (RNA)

What is your company's current state?

Is there enough capacity (corporate and/or user's personal)?	**Yes** – User internet speeds and applications profile are known. The corporate service side capacity is large enough to meet the increased demand.	**Partially** – There should be sufficient bandwidth but there are some concerns. Corporate strategy allows for staggered work hours.	**No** – There are known capacity limitations and there is no mapping of user Internet speeds. Situation translates in high number of support incidents.
Have you given network priority to your business- critical applications?	**Yes** – There is application priority and traffic split- tunneling protection for delay-sensitive and mission- critical applications. Trusted bulk Internet traffic is diverted locally at the end-user side.	**Partially** – There is network priority given to voice and video applications. All traffic crosses the central hub and corporate Internet proxy cluster.	**No** – All traffic is treated equal. Voice and bulk traffic cross the corporate proxy. Under congested conditions there is a high number of user complaints.
Do you have the right monitoring tools in place?	**Yes** – There is application, licensing, network and end- user capacity monitoring in place, and they are below the platform's max sessions count.	**Partially** – There are some gaps in our monitoring systems. There are concerns about the impact of those to scale the remote network access service.	**No** – There's no good visibility, and the current platforms could be close to max utilization. We cannot monitor user Service Level Agreements (SLA).
Have you deployed a resilient Integrated Security Solution (inspection, firewall, advanced malware detection, site-to-site VPN, etc.)?	**Yes** – The service platforms have all required security components and have all required dimensioning and resiliency in place.	**Partially** – There are a few security components missing. The central VPN concentrators have no possible redundancy.	**No** – The only firewall is not redundant and provides multiple services to the organization.

Devices Requirements

RNA Client  RNA Server  Virtual Office Router  Teleworker Router  Office Extension Access Point 

Basic	Optimized	Fault Tolerant
Standalone Firewall	High availability (active/standby)	Fully redundant (active/active)

Collaboration Solution

Collaboration consists of a collection of tools and applications that rely on the previous categories to be effective. An identified risk in any of the previous sections corresponds to a risk within the collaboration environment.

Outcomes

- **Identify** all adjacent architectures and align functionality against success criteria (network, security, etc.)
- **Identify** and account for all external collaboration scenarios and baseline them against compliance and regulatory requirements
- **Facilitate and centralize** targeted training sessions for remote work policy and procedures
- **Incorporate** Single Sign On for authentication

Good Practices

- Incorporated holistic plan that incorporates people, process, and technology
- Decoupled workplace and task fulfillment
- Connected and empowered workforce

Related offers:

- Pop up sites
- Virtual Visitation
- Secure Remote Worker
- Cisco DNA Spaces
- Webex Contact centre
- Virtual education
- Business Resiliency Strategy and Roadmap

Capabilities


Calling


Meeting


Messaging


Files

Collaboration Solution Cont.

What is your company's current state?

Are your workers familiar with the targeted collaboration tools and capabilities?	**Yes** – The workforce is familiar and proficient in all the targeted tools and capabilities.	**Partially** – There are a subset of workers that need to be trained on the targeted toolset and capabilities.	**No** – Our workers will need to be trained on the targeted toolset and capabilities.
Are your workers familiar with work-from-home policies and procedures regarding remote collaboration?	**Yes** – The policies have been distributed and are understood by the workforce.	**Partially** – Policies and procedures have been created but need to be better understood by the workforce.	**No** – Policies and procedures have not been distributed are not fully understood by the workforce.
Does your remote workforce have the ability to collaborate with partners and/or clients as needed?	**Yes** – All of our existing tools and capabilities allows us to effectively collaborate with our partners and/or clients as necessary.	**Partially** – Some of our existing tools and capabilities allow us to collaborate with our partners and/or clients as necessary.	**No** – Our existing tools and capabilities do not allow us to effectively collaborate with our partners and/or clients.
Are your targeted collaboration tools and capabilities in compliance with all company and regulatory policies?	**Yes** – Our targeted collaboration tools and capabilities are compliant.	**Partially** – Some of our targeted collaboration tools and capabilities are compliant.	**No** – Our targeted collaboration tools and capabilities are not compliant.

Device Requirements			Personal	Group	Extended
Laptop 	Mobility Devices 	Headset 	• Email • Telephony • Video • IM/Presence	• Video • Web Conference • File Sharing	• Video • Streamed Event • File Sharing

Thank you for reading

Work From Home and Business Continuity Strategy Self- Assessment

Get CX Experts to help build a customized and transformational
Business Resiliency Strategy and Roadmap