

FORVIS

WEBINAR

Internal Controls & Working From Home

March 26, 2024

Meet the Presenters



Wil Crawford
Partner, Assurance
Jackson, MS
wil.crawford@forvis.com



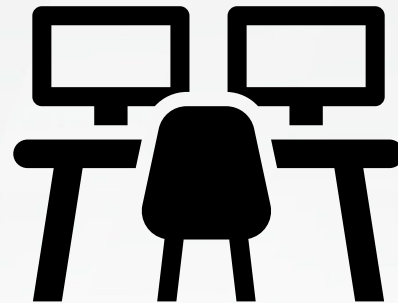
Raj Kapur
Director, Nonprofit Advisory Services
Metro D.C.
raj.kapur@forvis.com

Learning Objectives

- Explain new risks in remote and hybrid working environments
- Identify unique IT security concerns when working from home
- Recognize the internal control challenges in a remote environment

McKinsey & Company American Opportunity Survey

Americans are embracing flexible work—
& they want more of it



McKinsey & Company

American Opportunity Survey

- McKinsey worked alongside the market-research firm Ipsos to query 25,000 Americans in spring 2022
- 25-minute, online-only Ipsos poll conducted on behalf of McKinsey between March 15 & April 18, 2022
- Adults aged 18 & older from the continental United States, Alaska, & Hawaii were interviewed online in English & Spanish

McKinsey & Company | American Opportunity Survey

Of job holders in the United States, 58 percent—the equivalent of 92 million people—say they can work remotely at least part of the time.

Availability of remote-work options, % of employed respondents (n = 13,896)¹

Offered remote work on a full-time basis

35

Offered remote work part-time or on occasion

23

Not offered remote-work opportunities¹

42



Number of workers, extrapolated²
55 million

36 million

66 million

Note: Figures may not sum, because of rounding.

¹Includes respondents who answered "I don't know" (1%).

²Of 158,105,000 employed people; US Bureau of Labor Statistics, Apr 2022.

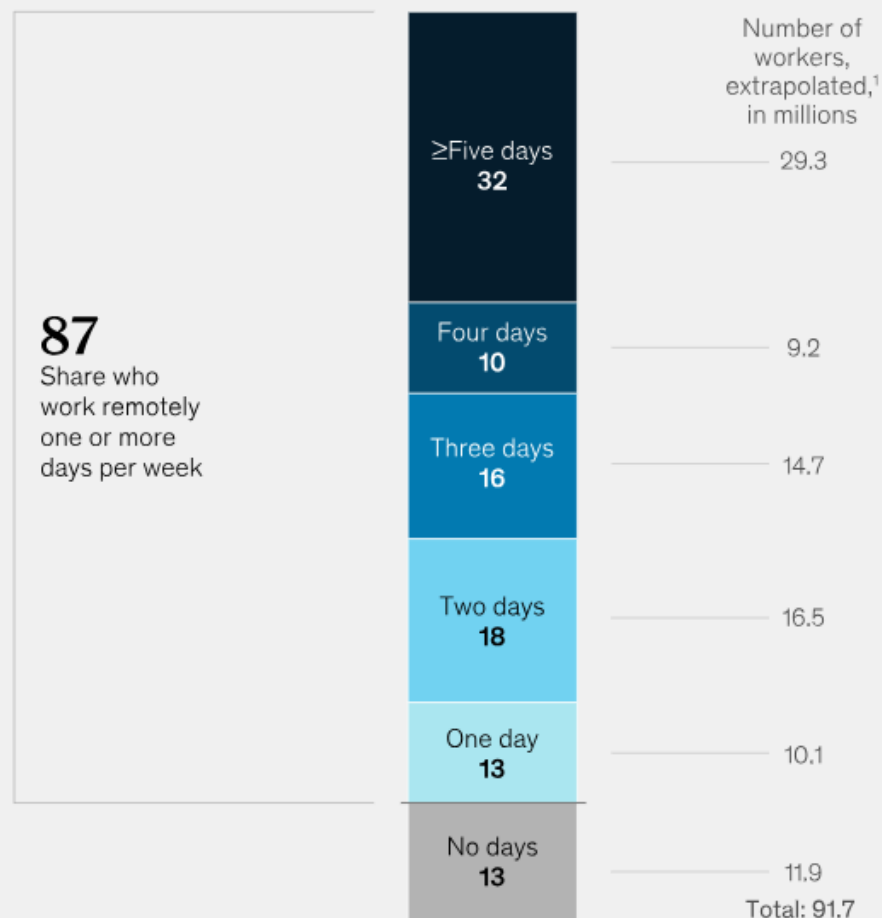
Source: McKinsey American Opportunity Survey Spring 2022

McKinsey
& Company

McKinsey & Company | American Opportunity Survey

Among employed respondents given the option to work remotely, 87 percent take employers up on that offer.

Days worked remotely per week, % of employed respondents with remote-work options (n = 13,896)



Note: Figures may not sum to 100%, because of rounding.

¹Includes 158,105,000 employed people; US Bureau of Labor Statistics, Apr 2022; 35% of respondents reported having the option to work fully remote, and 23% reported having the option to work from home on occasion/part-time.

Source: McKinsey American Opportunity Survey Spring 2022

Takeaways

Most industries support some flexibility, but digital innovators demand it.

Job seekers highly value having autonomy over where & when they work.

Employees working flexibly report obstacles to peak performance.

Journal of Accountancy

**Future C-suite
leaders banking
on continued
hybrid work
model**

August 9, 2023

Changes necessitated by the pandemic & enabled by the constant march forward of technology have altered the way we work forever, so it's not surprising that an attempt to return to the pre-pandemic norm could come at a cost to workforce morale at the least & quite possibly to the talent pipeline itself.

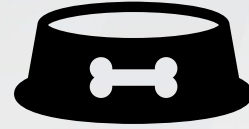
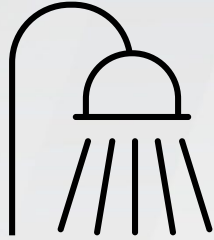
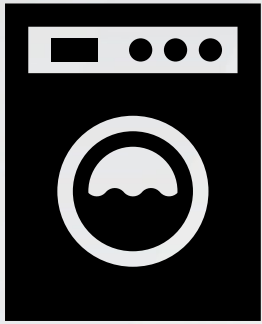
**Flexibility is the
new normal**

Challenges When Working From Home



FORV/S

FORVIS is a trademark of FORVIS, LLP, registered with the U.S. Patent and Trademark Office.



Remote Working Distractions

- Family/Friends Interruptions
- Social Media, Email, & Online Entertainment
- Pet Distractions
- Outside Noises
- Housework
- Cooking
- TV



Journal of Accountancy

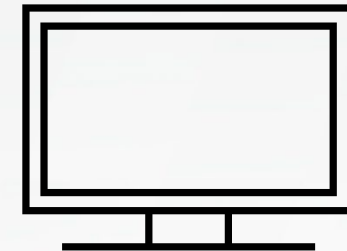
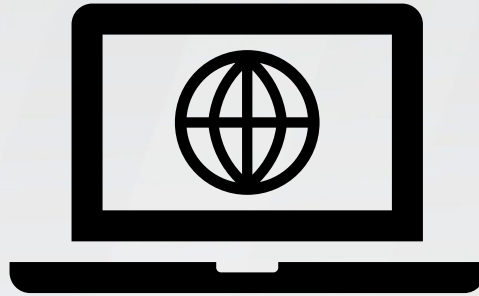
8 tips for fending off digital distractions

- 1) Block off time to focus on specific tasks – use 50 or 90 minute intervals
- 2) Consider turning off your notifications
- 3) Find a system of prioritizing your inbox
- 4) Manage your calendar efficiently
- 5) Articulate your communication preferences
- 6) Strive for consistency over speed
- 7) Schedule your communication
- 8) Take real breaks



COVID-19, College Students, & Distractions

Defining a new
baseline of
distraction



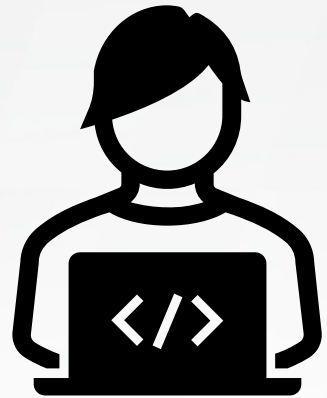
FORV/S

Baseline of Distraction



- What is your baseline of distraction/focus when working from home (as a %)?
- Is it different from when you work in the office?
- Have you ever multi-tasked during a Zoom meeting?
- Multi-tasking is a **MYTH**

IT Controls When Working From Home

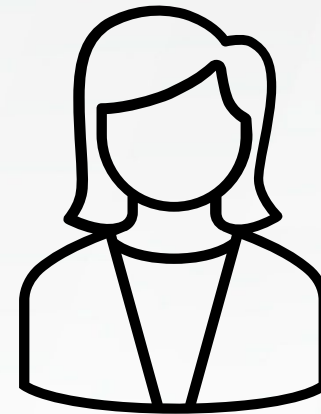


FORV/S

FORVIS is a trademark of FORVIS, LLP, registered with the U.S. Patent and Trademark Office.

Key Internal & IT Controls Around Remote Work

- Employee Security Awareness Training
- Segregation of Duties
- Authorization/Approvals
- Reconciliation/Review
- Physical Security
- System Access Controls
- Data Backup/Encryption
- Limit Local Administrator Access
- Patch Management



Information Systems Audit & Control Association [ISACA]

Five Key
Considerations
When Securing a
Work-from-Home
Workforce

July 6, 2020

Working from home creates opportunities for new threats & vulnerabilities that must be evaluated ... attackers quickly adapted their methods to leverage the inherent weaknesses created in work-from-home environments ...

With tools such as the Shodan search engine, which can be used to identify exploitable Internet-connected devices in home networks, adversaries have systematically been attacking home routers, Internet of Things (IoT) devices, *i.e.*, smart televisions, digital video recorders [DVRs], printers, & other computing devices that can be used for attacks such as denial-of-service (DoS), ransomware, malware injections, & others.

To combat these threats, it is important to apply the same vulnerability analysis techniques used in enterprise environments using existing case studies & thoughtful analysis.

ISACA

Five Key Considerations When Securing a Work-from-Home Workforce

July 6, 2020

Conducting virtual site reviews for high-risk or concerned workers is essential ... Audit & security professionals can help high-risk workers identify & remediate security & privacy deficiencies in their work-from-home environments using virtual risk & security site reviews.

By having a guided & targeted video conversation with the home worker, security professionals can help remote workers identify & mitigate risk in their home work areas.

Some common risk examples that are often identified in virtual site reviews are sensitive materials scattered across a work environment, windows where unauthorized individuals may be able to see information displayed on screens without the worker's knowledge, open work areas where family members & random individuals could easily overhear conversations & view materials without restriction, & items that may divulge private details about a worker or their family that an adversary could use as part of a targeted attack.

ISACA

Five Key Considerations When Securing a Work-from-Home Workforce

July 6, 2020

Incorporating work-from-home considerations into security awareness training benefits everyone ...

Security awareness training should be updated to reflect remote-work-specific guidance & requirements. If an organization can introduce content to the home worker that is beneficial to them both professionally & personally, they are more likely to follow & even embrace the guidance.

As a result, remote workers will often intuitively increase their overall security posture while operating in a work-from-home environment. For example, helping users understand the importance of keeping their home-network-connected devices updated with the latest security patches or ensuring they are using strong encryption & passwords on their home wireless network can strengthen their overall security posture.

ISACA

Five Key Considerations When Securing a Work-from-Home Workforce

July 6, 2020

Promoting good information security hygiene for work-from-home environments reduces threats. Good information security hygiene focuses on foundational & typically unsophisticated capabilities that must be regularly attended to & can dramatically reduce the threat & vulnerability surface area of a remote work environment. Examples of security hygiene activities that both an organization & a remote worker can actively follow include the following:

- Patching, updating & configuration security-hardening of an organization's technical assets & the technical assets operating on common networks in the work-from-home environment
- Following clean desk, work area, & whiteboard practices where the environment is cleaned at the end of each workday
- Consistent use of privacy screens on monitors & displays where sensitive data are or could be displayed
- The use of segmented work areas from the general home environment with lockable doors or barriers to limit unauthorized individuals from entering the work-from-home area at inopportune times
- Regular changing of passwords & use of multifactor authentication, where possible, for access to enterprise & home environment technology assets
- Logging off or engaging password protection on computing displays whenever they are left unattended (instead of waiting for standard timers to engage)

IT Control Risks With Remote Work

- **Social Engineering/Cyberattacks**

- 1) **Phishing**

- An online scam enticing users to share private information using deceitful or misleading tactics.

- 2) **Ransomware**

- Ransomware is a type of malware identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided.

- 3) **Remote Desktop Protocol (RDP) Hacking**

- Common way for hackers to access valuable password & system information on networks that rely on RDP to function.

- 4) **Denial-of-Service (DoS) Attack**

- Occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

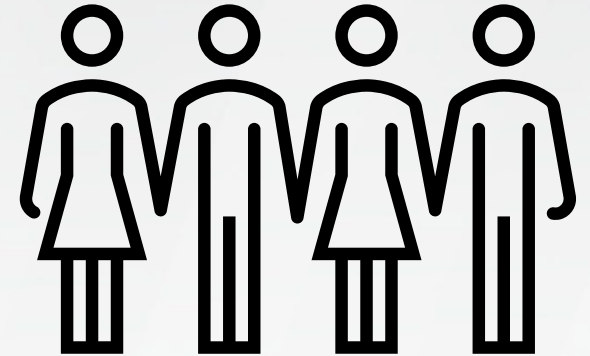
- 5) **Zoombombing or Zoom Raiding**

- Type of cyber-harassment in which an individual or a group of unwanted & uninvited users interrupt online meetings over the Zoom video conference app.

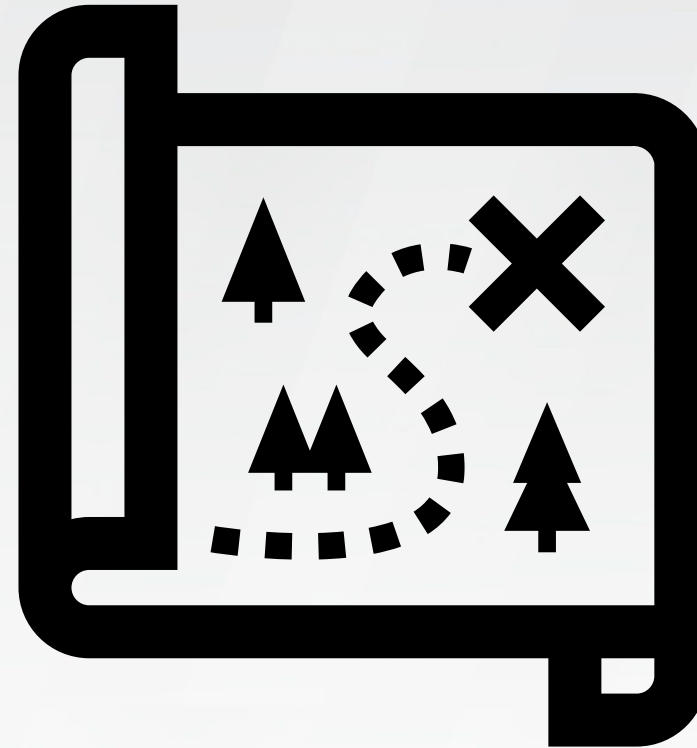


What Can Team Members Do to Manage Technology Risk?

- Maintain Consistent Communication With Managers & Team
- Be Skeptical of Emails, Links, Attachments, Apps, & Phone Calls From Unknown Parties
- Don't Install Unauthorized Software or Suspicious Apps on Company Devices
- Don't Allow Others to Use Company Computer or Accounts
- Don't Permit Unknown or Insecure Devices to Connect to the Same Network—Wireless or Otherwise—as Your Company Devices
- Follow Company Policy & Process for Validating Customer/Vendor Identity
- Don't Share or Change Company Information Without Approval
- Don't Bypass Company Policies or Processes



Internal Controls, Working From Home, & a Conceptual Framework



FORV/S

Internal Controls, Working From Home, & a Conceptual Framework



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

FORV/S

The COSO Cube

How does working from home impact the standard elements of the COSO Cube?

What elements are now more difficult?

What elements are now more important than before?



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

The COSO Cube

- Impacted?
 - The tone at the top
 - The human element
 - Staff education & training
 - Commitment, loyalty, dedication, etc.
 - Tenure
 - Turnover



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

FORVIS Audit Level 1 Training on Internal Controls

What We Do?

What Can Go Wrong?

What Do We Do About It?

Understand Process

How do transactions get recorded in the financial statements?

Assess Risk

How can material misstatements occur in the financial reporting process?

Evaluate Design of Controls

Do controls, individually or in combination, prevent or detect & correct material misstatements?

Process Re-engineering

- Organizations have altered their implemented processes, procedures, & internal controls to adapt to the remote nature of business. There may have been things that were previously done in person or that utilized paper copies. Organizations can't bypass controls just because it seems difficult in a remote world. Re-engineer processes where necessary & possible.



Illinois CPA Society

Internal Controls in a Remote World

Ten steps to developing robust remote internal controls

#1: Reexamine segregation of duties.

#2: Take advantage of technology.

#3: Track, document, & confirm.

#4: Know your data.

#5: Find new lines of communication.

#6: Assess cyber risk.

#7: Get leaders involved.

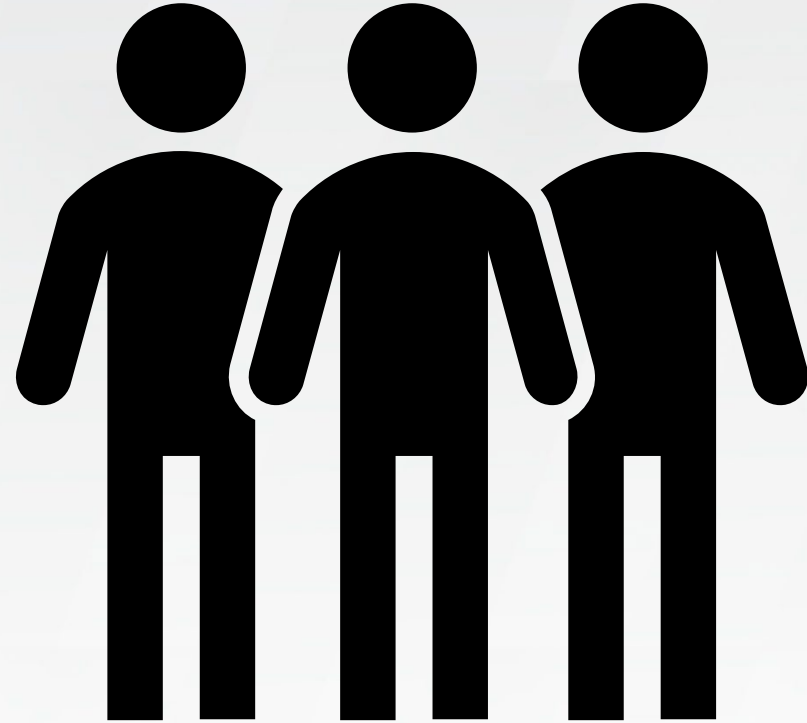
#8: Draw attention to ongoing monitoring.

#9: Remember the human element.

#10: Communicate with your clients.

In Closing ...

The Human Element



FORV/S

Fast Company

A psychologist explains how working remotely impacts your relationship with your boss

August 18, 2023

Five recommendations for cultivating a good relationship with your boss when working remote:

- 1. Be super clear outlining your goals & objectives:** Nudge them into managing & measuring your performance for what you deliver.
- 2. Keep them frequently updated on progress:** Let them monitor your progress as often as they can or want to. Ideally, give them access to any live or real-time data on how you are performing.
- 3. Schedule the necessary in-person time:** Meeting in person is key to recharge trust & reinvest in the emotional & psychological connection that can make online meetings more tactical, operational, & task-oriented.

<https://www.linkedin.com/pulse/psychologist-explains-how-working-remotely-impacts-your-relationship/>

Fast Company

A psychologist
explains how
working remotely
impacts your
relationship with
your boss

August 18, 2023

Five recommendations for cultivating a good relationship with your boss when working remote:

4. Don't disconnect from the team: Whether your colleagues & teammates are working from home or at the office—especially if they are mostly at the office when you are not—be sure to keep in close contact with them, understanding not just the ins & outs of their working routine but also whichever personal or social aspects they are willing to share. Being physically distant doesn't mean you must be emotionally disconnected.

5. Be open to change: If there is evidence to suggest that working remotely has led you to be less effective than you were at the office, accept it & offer to return. Unless, of course, you are determined to avoid it (in which case you may consider changing jobs altogether).

Questions?

FORV/S

FORVIS is a trademark of FORVIS, LLP, registered with the U.S. Patent and Trademark Office.

Thank you!

forvis.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by FORVIS or the author(s) as to any individual situation as situations are fact specific. The reader should perform its own analysis and form its own conclusions regarding any specific situation. Further, the author(s) conclusions may be revised without notice with or without changes in industry information and legal authorities. FORVIS has been registered in the U.S. Patent and Trademark Office, which registration is pending.

FORVIS

Assurance / Tax / Consulting