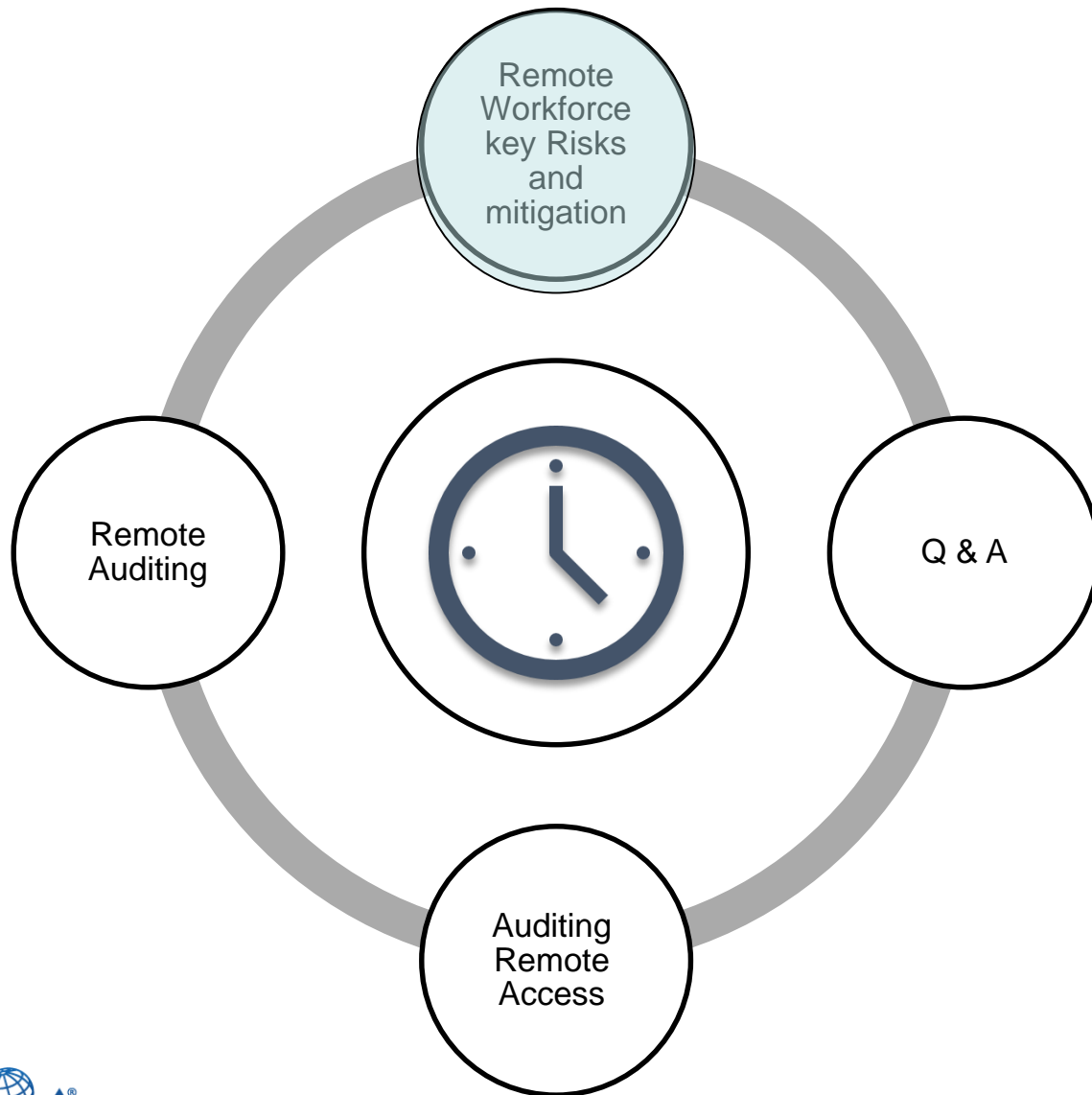# Remote Workforce

Lior Segal, Advocate, CPA, MBA, CIA, CRMA, EQA, CRISC, CDPSE

Chief Audit Executive, Bezeq
Director, Secretary, Treasurer, IIA Israel

Webinar for IIA Croatia
15th July, 2021

Agenda

Remote Workforce key Risks and mitigation

Remote Auditing

Q & A

Auditing Remote Access

Lior Segal – Few words about me

- Over 20 years of experience in Audit, Risk and Control fields in Public companies, mostly on management positions
- Chief Audit Executive at Bezeq, Israel largest Telecom operator
- Director, Treasurer and Secretary at IIA Israel
- Teaches on various training and professional courses, including in Academics
- Audit Committee Member in a non-profit organization
- Bachelor of Law (LL.B), Bachelor of Accounting (B.A), M.B.A, dual majors: Finance& Accounting and Strategy& Entrepreneurship, Bachelor of Comprehensive Audit Studies, CIA, CRMA, CRISC, CDPSE, EQA (External Quality Assessor)
- An Advocate and a CPA
- Married to Karen, father of two sets of twins
- Likes running, travelling, SKI, Playing Tenor Saxophone and teaching\ lecturing

Nowadays Challenges for Internal Auditor Are Complicated*

Challenges in the organization*

- Resources, resources, resources

- Different stakeholders with diversified demands

- Control, risk management and compliance – audit fatigue

Challenges outside the organization*

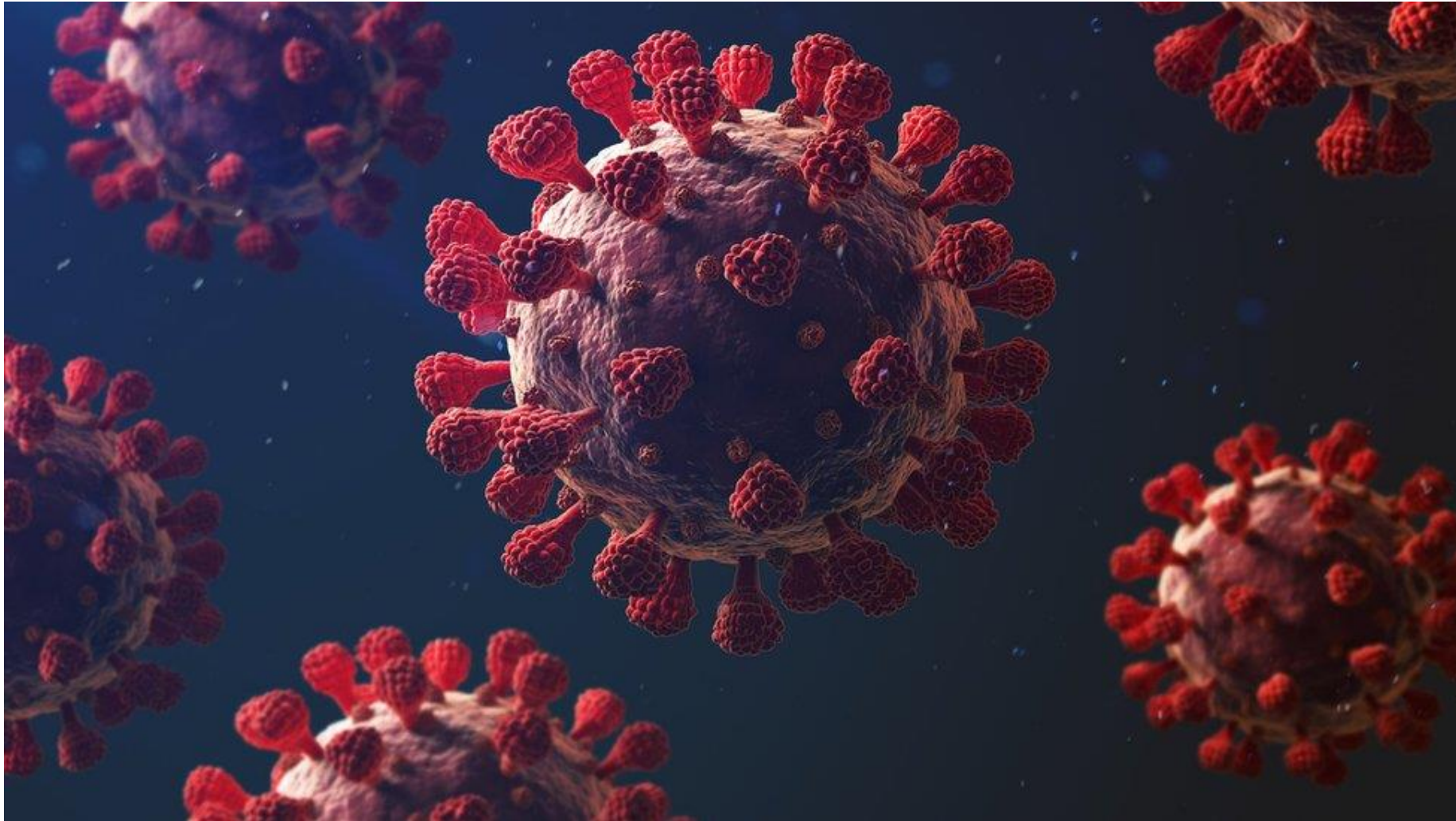- Increased compliance requirements

- Corporate governance development

- Rapid technology development

- Emerging risks, such as COVID and Work from Home

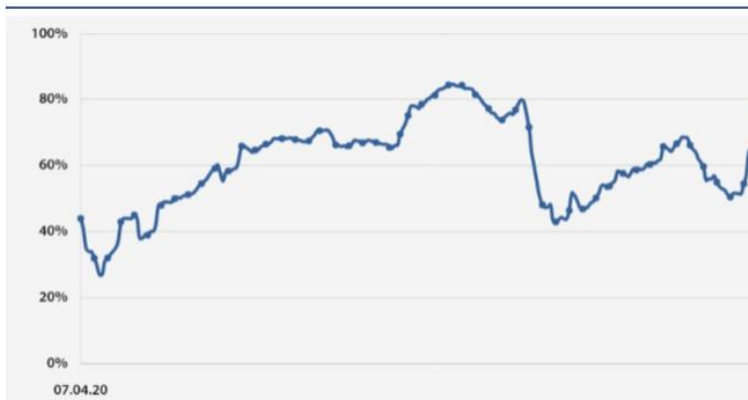*** There are more challenges**

COVID-19 Surprised (Most of) Us
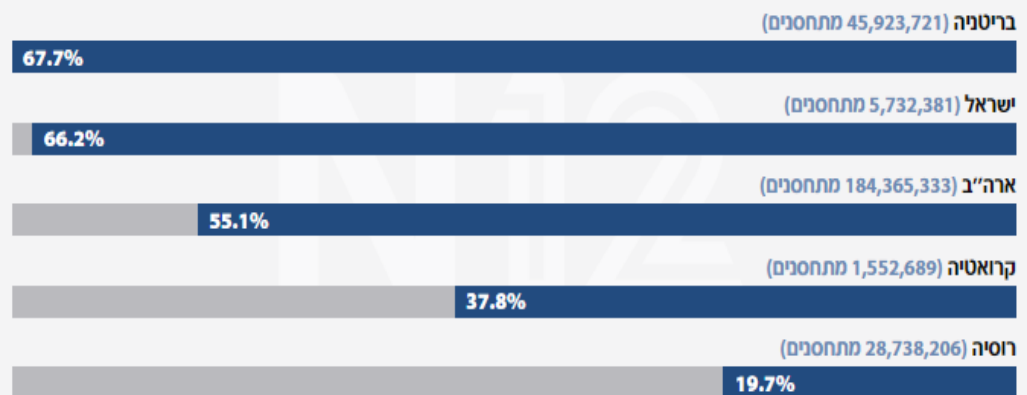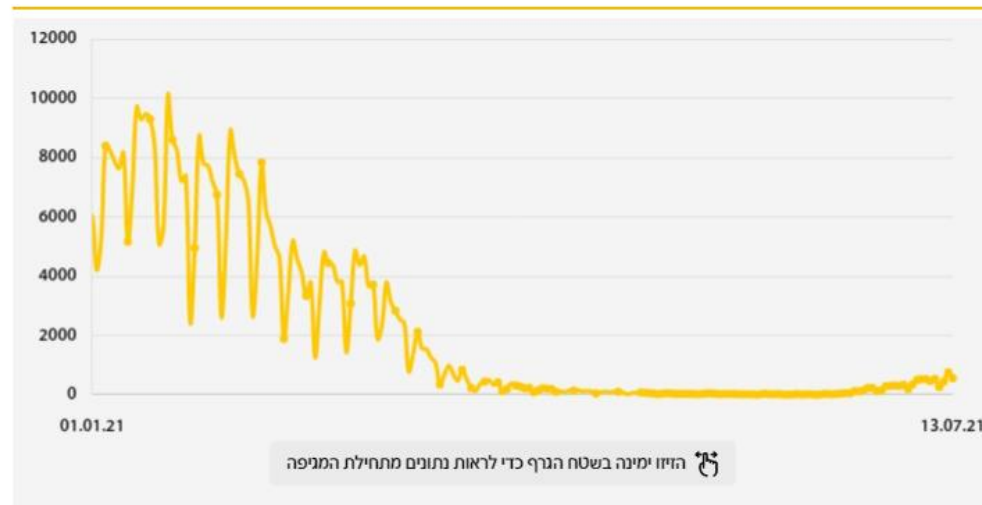
COVID 19 in Israel- Selected figures

Israel has gone through 3
lockdown (03/20, 09/20,
01/21) and a continuous set
of restrictions, an Increase is
happening lately

Number of infected daily

הזיזו ימינה בשטח הגרף כדי לראות נתונים מתחילת המגיפה

Getting back to Normal Index

בריטניה (45,923,721 מתחסנים)	67.7%
ישראל (5,732,381 מתחסנים)	66.2%
ארה"ב (184,365,333 מתחסנים)	55.1%
קרואטיה (1,552,689 מתחסנים)	37.8%
רוסיה (28,738,206 מתחסנים)	19.7%

גרה של 12N, שנבנה בעזרת יזום אריאב ויוסי קפציק, מציג באמצעות שורה של אינדיקטורים באיזה מצב נמצא המשק הישראלי, בהשוואה לשנה שקדמה למשבר הקורונה

https://ourworldindata.org/covid-vaccinations

We Did Work Remotely Before COVID-19, But…

- Although seems otherwise, remote workforce is not a new issue

- Organizations gave their employees the flexibility to work from home before February 2020

- **However, COVID-19 accelerated this significantly, and organizations began to understand, even 15 minutes into the pandemic:** the New Normal will not be the same

Remote Workforce has not been a New Risk at My Company (Bezeq)

COVID-19 forced almost all the employees in the globe to work remotely

So, Let Us Discuss Some Risks and Challenges of Remote Workforce

Work from Home Requires Adjustments, Not All of Them Were Possible When COVID Hit Us, Abruptly

- Mapping and prioritization
- Employees Readiness
- Security
- Channeling Policies and procedures
- Remote Workforce
- Patience and listening
- Technology readiness
- Culture
- Management and measurement

Significant Threats in Remote Access-Security-wise

Loss of data and **data leakage**

DOS attacks using remote connections

User Access privileges outside the "**need to know**" principle

Attack of the identification mechanism, by guessing password and Brute force attacks

Receiving of malicious files via email

Entrance to the organizational network by an **unauthorized party**, that can take advantages of security vulnerabilities (e.g., anti virus, operating systems, remote access) and lack of hardening)
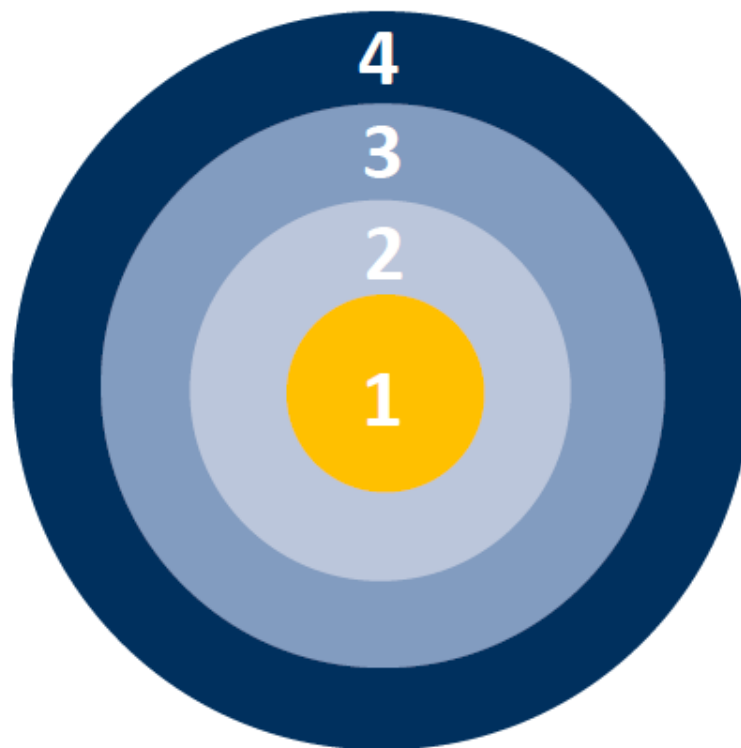
Protection is required in all the Layers

4. User

3. Network/infrastructure

2. Application

1. Database

In the current work-from-home environment, companies need to ensure effective security is still in place with each ring.

Source: Fastpath Solutions LLC

And Employees behavior- A Major Threat

- ## According to Cyber Arc*
  - ### Convenience Often Outweighs Security
    - 93% have reused passwords across applications and devices
    - 29% admitted that they allow other members of their household to use their corporate devices
    - 37% insecurely save passwords in browsers
  - ### Are Current Work from Home Security Policies Enough?
    - While 94% of IT teams are confident in their ability to secure the new remote workforce, 40% have not increased their security protocols despite the significant change

- ## According to "Absolute"**, over 60% of the data breaches exposed are linked to a security patch available but not installed on a timely basis

Security Recommendations for Remote Work Force

- Israel National Cyber Directorate ("INCD") published a memo focusing on remote work force risks and mitigation
- Their suggestion is to protect the organization on 3 areas

Protecting the Network

Employees Awareness

Employees Protection

INCD's Recommendations - Protecting the network

Connect via a permanent device

Remote access privileges to essential folders

Separate access to emails and access to folders\ servers\ assets

Removing access of employees to systems and interfaces they do not require

Periodic review Back-ups to all the devices and to the data

Define enforcement policies on Passwords, periodic change

Limit remote connection time (session)

Fine tune of firewall rules and provide logs

Define privileged countries allowable for connectivity

Prevent access to code lines

Access via terminal server

INCD's Recommendations - Employees awareness

Lock the device with a strong password

Automatic lock the computer after a determined time away from the computer

One email for work-only and another for a private use

Improve the security level of easy-to-hack home router

Automatic software updates and/or instruction of employee how to install them

Raise the awareness regarding Phishing attacks done in all the channels, Private and Business

INCD's Recommendations - Employee Protection

All the devices the employees use are locked in password

Update anti-virus program

Initiate a process to detects different viruses and threats

Updated Firewall software

A secure and private VPN connection between the employee and the organization resources

Two or multi factor authentication
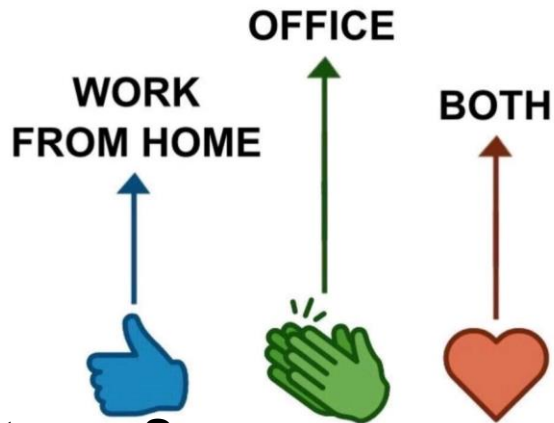
Automatic software updates for all software on the devices

PROTECTION OF EMPLOYEES

Is the Pandemic Reflecting a Temporary Situation or Are we Heading towards a "New Normal"?

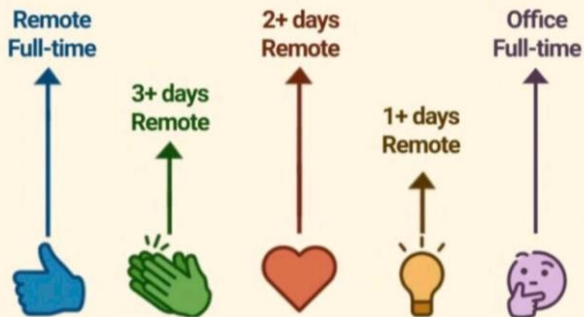# Interesting Surveys I came Across in LinkedIn

WHAT WOULD YOU PREFER?

OFFICE

WORK FROM HOME

BOTH

Stauna Soanes

Reactions

7%	35%	56%
2,301	11,380	18,336

May 2021

9%	34%	57%
8,790	35,442	58,759

3%	5%	15%	27%	50%
233	296	962	1,730	3,256

Where do you want to work after Covid?

Remote Full-time

3+ days Remote

2+ days Remote

1+ days Remote

Office Full-time

Todd Laduron

IIA ISRAEL INSTITUTE OF INTERNAL AUDITORS

What would you prefer?

Work From Home

Office

JobAlert.co.in

Job Alert Celebrate

25%	75%
952	2,847

Surprised?

19
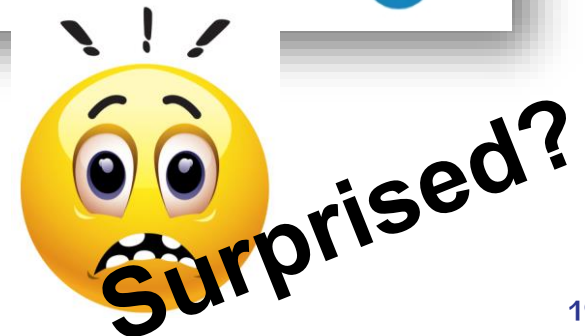
Another Perspective

How would you rate your level of productivity while working remotely?

60%	
50%	48%
40%	
30%	30%
20%	22%
10%	
0%	

■ Higher Productivity   ■ Same Productivity   ■ Lower Productivity
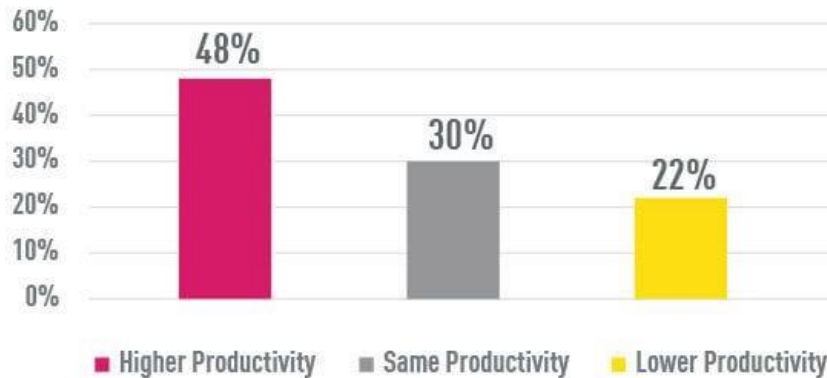
/https://blog.checkpoint.com

Thrives in the office

Thrives when working from home	YES!	Yes	Neither/nor	No	NO!
YES!	54%	26%	24%	28%	41%
Yes	27%	42%	36%	42%	24%
Neither/nor	5%	18%	28%	17%	17%
No	11%	12%	9%	10%	13%
NO!	3%	2%	3%	3%	5%

*Working from home: Survey results on the new normal

Increased Productivity Employees who are more satisfied with their jobs tend to be more productive. The Stanford study finds that employees who work at home experience a 13% boost in productivity versus those who work in a traditional office. Employees who telecommute work the equivalent of 1.4 more days per month than do their office-based counterparts, according to a 2020 study by online employment company Airtasker.

* The 4 pillars of remote work for Audit Teams, Ken Harmon, 24/6/21

Agenda

Remote Workforce key Risks and mitigation

Remote Auditing

Q & A

Auditing Remote Access

לשכת המבקרים הפנימיים IIA ישראל (חל"ץ)
IIA ISRAEL-INSTITUTE OF INTERNAL AUDITORS
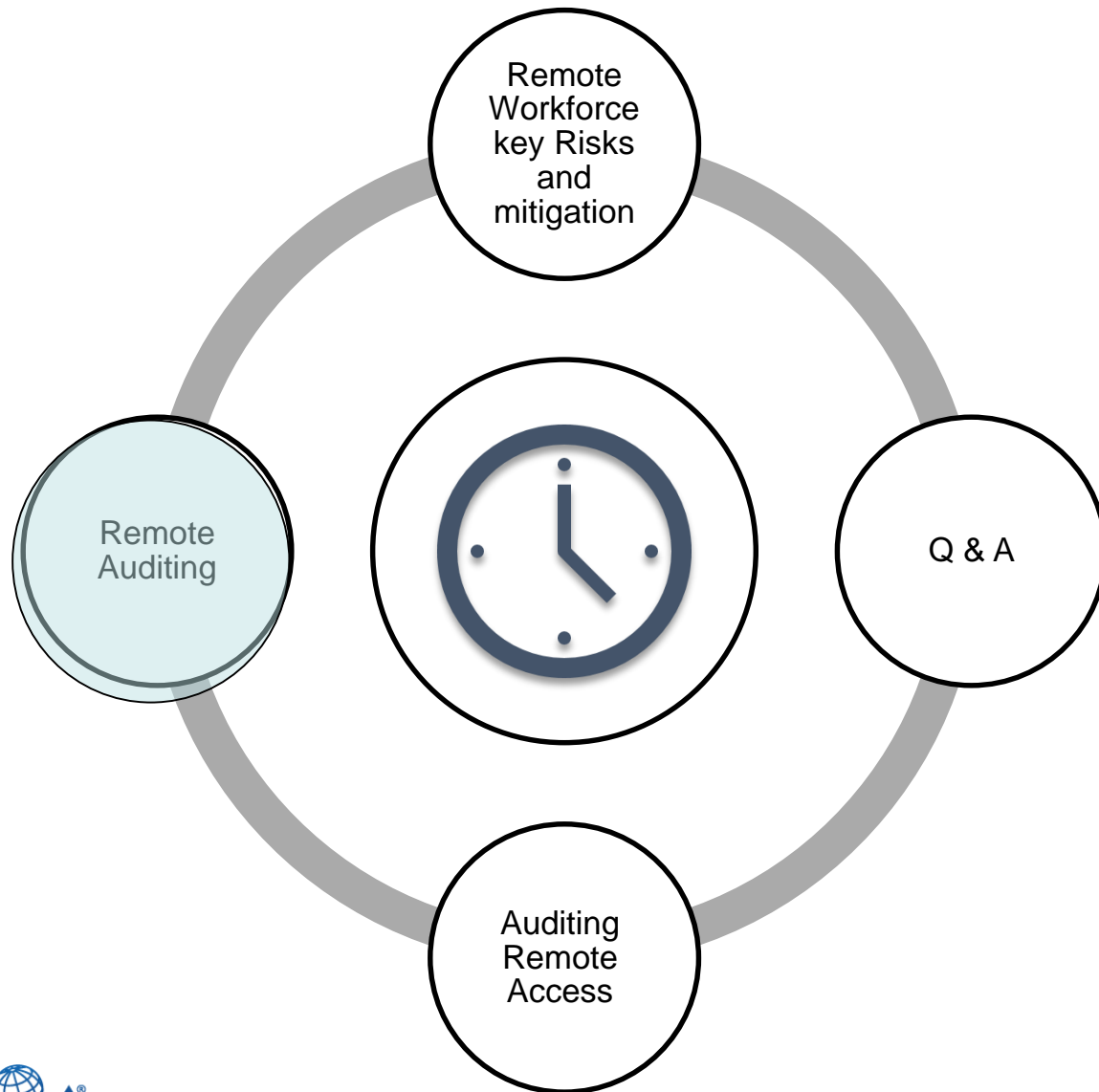
COVID-19 Raised Some Questions About Audit

What is Needed in Order to Effectively Audit Remotely

Arrange the Logistics

- Equipment
- Software
- Policy and Procedures (including remote work policy)

Communication with Stakeholders

- Within the audit unit
- Audit team engagement team, throughout all phases of regular audit
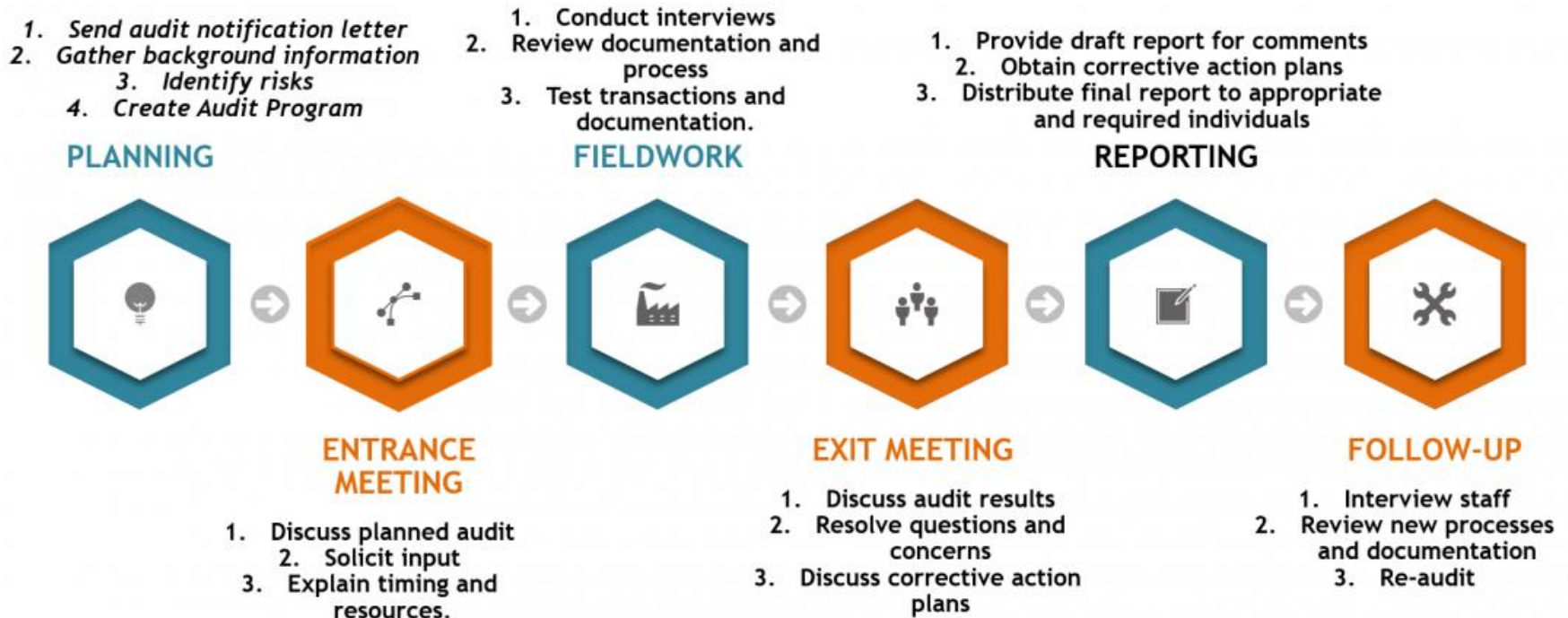- Auditees
- Chairmen of Audit Committee
- Management

Set Expectation inside the team

- Develop Formal Policies for remote work
- Discuss work hours and availability
- Set "check-in" calls- you can utilize ZOOM\ TEAMS\ WebEx

Expect the Unexpected

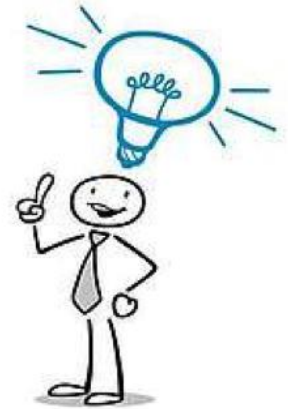- It is the same audit process, but different

לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA ISRAEL–INSTITUTE OF INTERNAL AUDITORS

We Understand Now- COVID'19's Changes Impacts all the Audit Process

1. Send audit notification letter
2. Gather background information
3. Identify risks
4. Create Audit Program

PLANNING

1. Conduct interviews
2. Review documentation and process
3. Test transactions and documentation.

FIELDWORK

1. Provide draft report for comments
2. Obtain corrective action plans
3. Distribute final report to appropriate and required individuals

REPORTING

ENTRANCE MEETING

1. Discuss planned audit
2. Solicit input
3. Explain timing and resources.

EXIT MEETING

1. Discuss audit results
2. Resolve questions and concerns
3. Discuss corrective action plans

FOLLOW-UP

1. Interview staff
2. Review new processes and documentation
3. Re-audit

Source: Summit Consulting

1+ Year into Covid-19, we are Still Partially\ Fully away from our offices

- We need to be very creative and to invent ourselves struggling with various issues, such as

How can we interview our Auditees?

How can we get to the field?

Which video conferencing app is best?

IIA ISRAEL-INSTITUTE OF INTERNAL AUDITORS

Again, Should We Audit in these Challenging Times?

To be, or Not To Be, That is The Question.

Remote Auditing- Pros and Cons

Pros

- A sense of normalcy- to the audit team and to the organization
- More Pure Audit hours
- Reduced travel costs
- Expanded use of specialists (not required to get to the Auditee)
- Better document reviews
- Audit burden is somehow mitigated
- Improved review confirmations as required in the Audit process

Cons

- Difficult to build relationship with auditees
- First-hand observations cannot be replaced\ can only be partially replaced
- Higher opportunities for fraud when you are not meeting the auditees
- Can be challenging if you are not a technology savvy

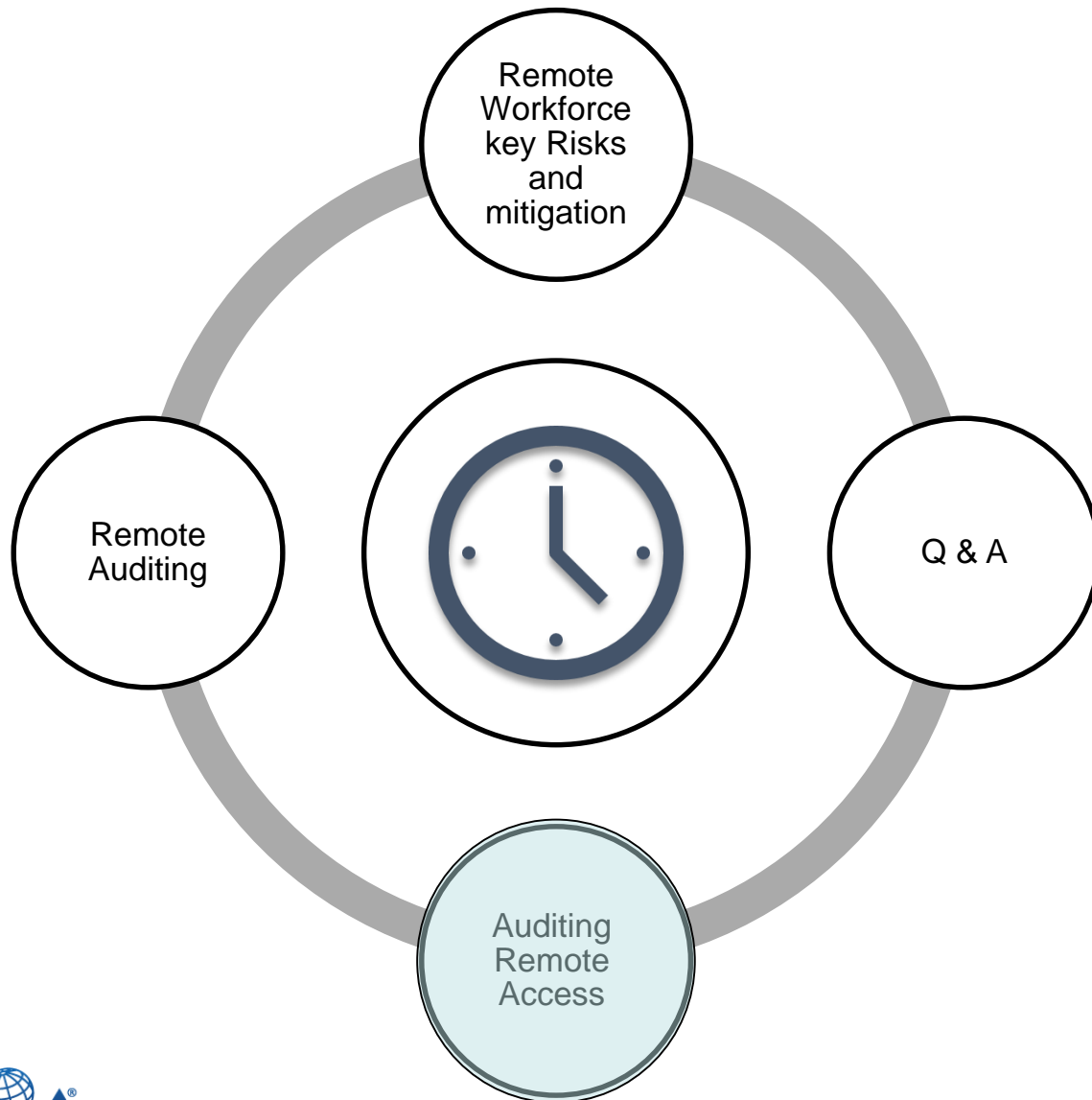**Due to the duration of the crisis- we have no other option but Audit Remotely**

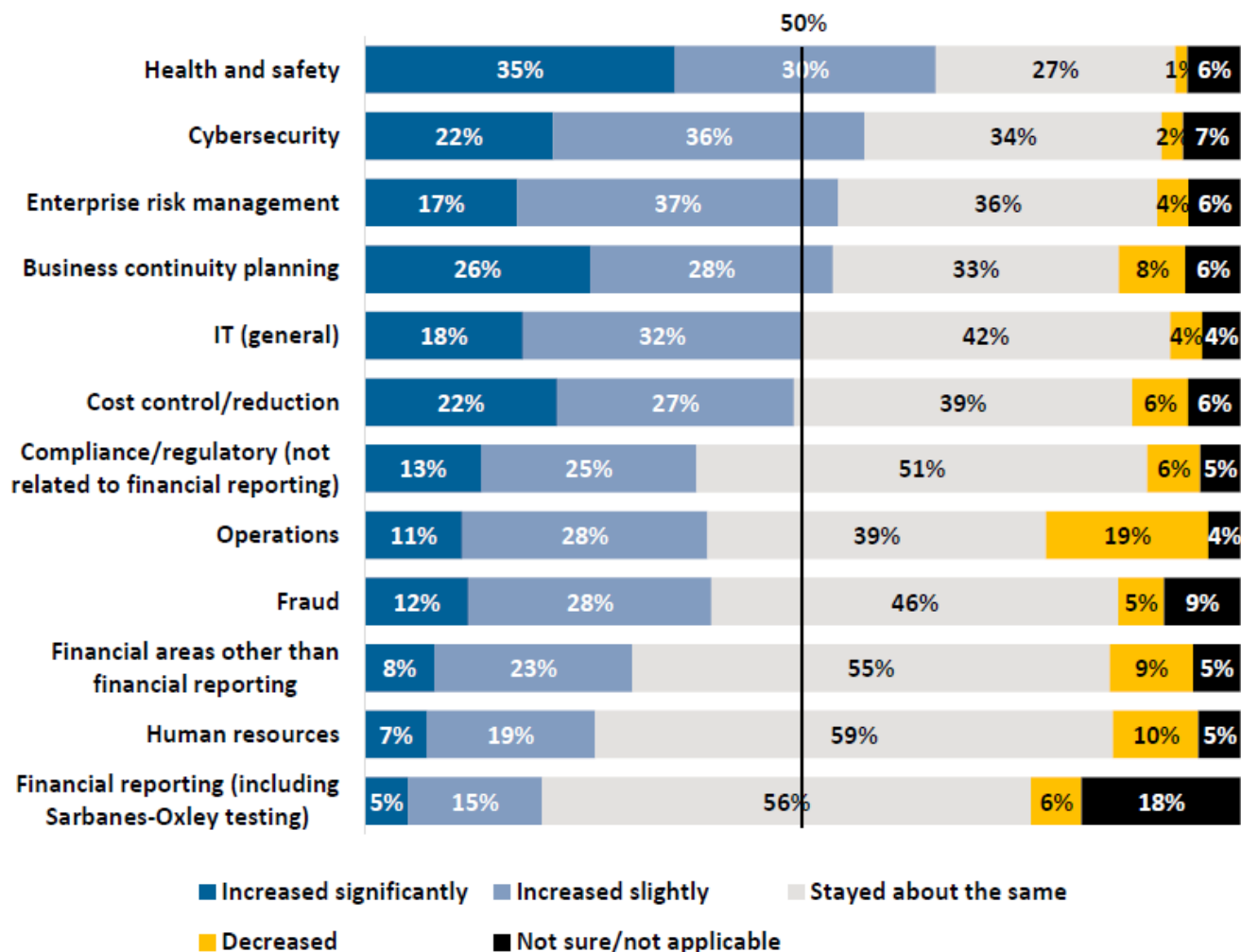# And - There Are Issues to the Retain, Also when the Pandemic Ends

Remote Working is Working!
So why not retain the Proficiencies
   and flexibility for the organizations
   and for the Internal Audit Function?

Agenda

Remote Workforce key Risks and mitigation

Remote Auditing

Q & A

Auditing Remote Access

לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA ISRAEL–INSTITUTE OF INTERNAL AUDITORS

Audit Focus Has Changed Due to COVID-19

Exhibit 10: Changes in Audit Focus Due to COVID-19 - All

Category	Increased significantly	Increased slightly	Stayed about the same	Decreased	Not sure/not applicable
Health and safety	35%	30%	27%	1%	6%
Cybersecurity	22%	36%	34%	2%	7%
Enterprise risk management	17%	37%	36%	4%	6%
Business continuity planning	26%	28%	33%	8%	6%
IT (general)	18%	32%	42%	4%	4%
Cost control/reduction	22%	27%	39%	6%	6%
Compliance/regulatory (not related to financial reporting)	13%	25%	51%	6%	5%
Operations	11%	28%	39%	19%	4%
Fraud	12%	28%	46%	5%	9%
Financial areas other than financial reporting	8%	23%	55%	9%	5%
Human resources	7%	19%	59%	10%	5%
Financial reporting (including Sarbanes-Oxley testing)	5%	15%	56%	6%	18%

Legend:
- ■ Increased significantly
- ■ Increased slightly
- ☐ Stayed about the same
- ■ Decreased
- ■ Not sure/not applicable

So, Should we audit Remote Access or not?

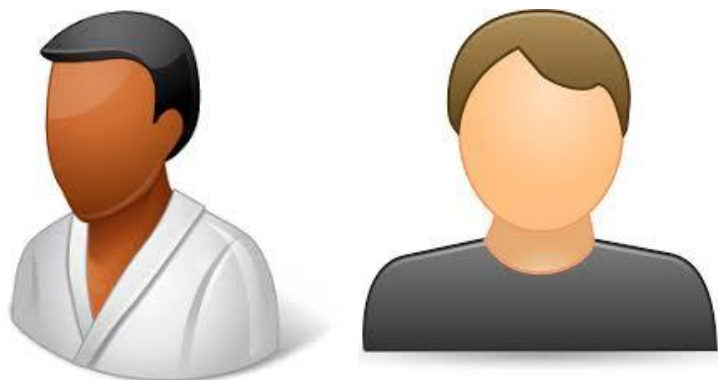# The Scope can be Endless in an organization with over 5,000 Employees and Many IT systems

Building a Dedicated Team

Internal Audit Consulting

Bezeq's Internal Audit

IS Consultant

Hacker

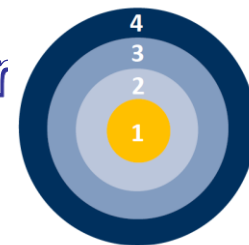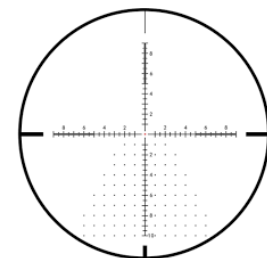**CAE**

IS Auditor

Focusing on the Following Areas

1. Governance

2. Remote Connection to Organizational Network

3. Remote Connection to emails

4. Equipment and Password used from remote

Pay Attention- this is not another Security\ Cyber Audit – this one is focused on the Remote access and work from home

1. Governance

- Although most of this engagement can be technical, Governance in relation to remote access should be a part
- Main steps

Remote access Governance

Audit step- Ensure corporate and security policies, including specific guidance to remote access, are being enforced

Audit step- Ensure business continuity and Disaster recovery plans practices are being followed

Audit step- Evaluate the logging/ reporting functions

Audit step- Ensure there is an effective methodology for event analysis

2. Remote Connection to Organizational Network - Background

- Many entities are required to have access to the organizational network

Human (employees, customers, suppliers)

Technology (applications)
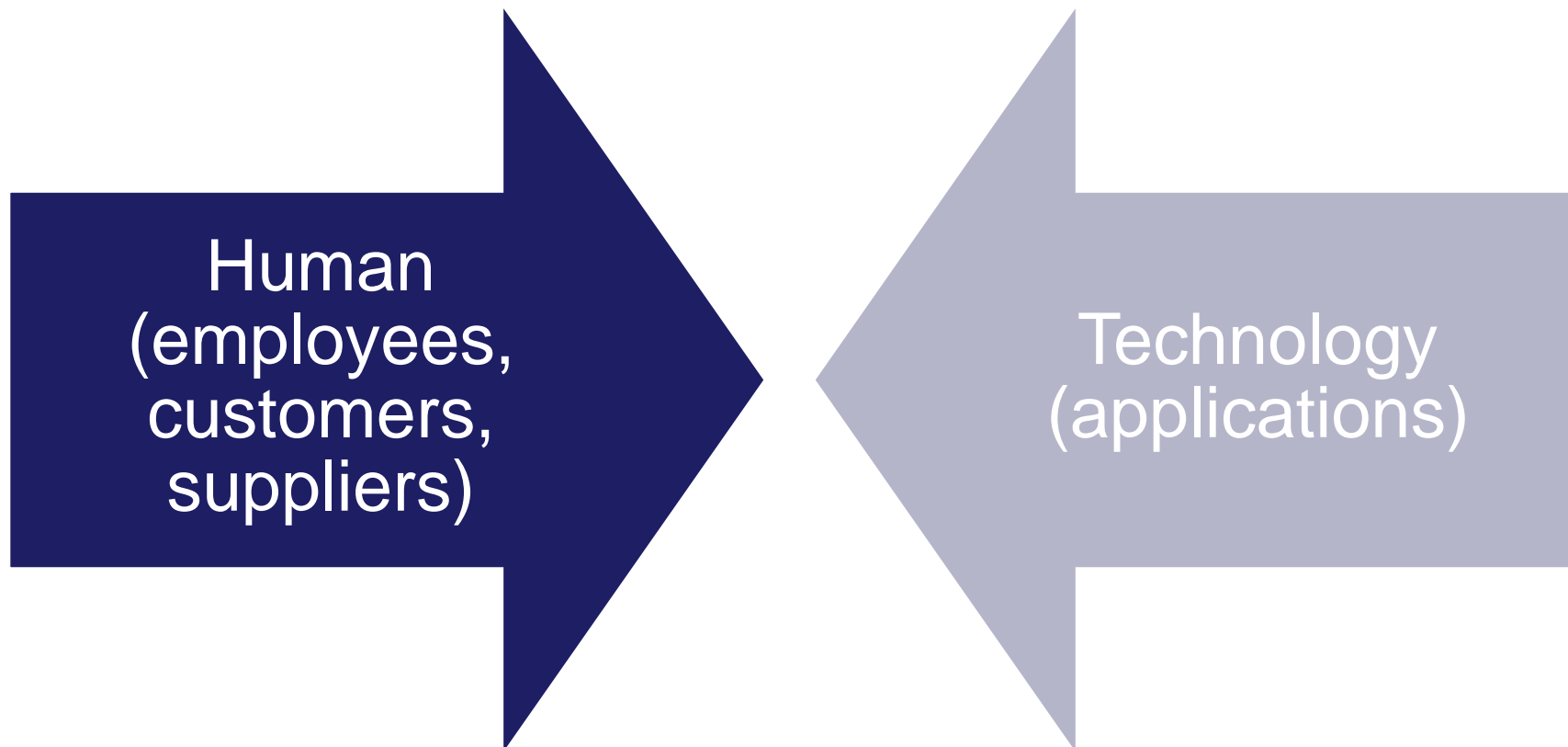
2. Remote Connection to Organizational Network - Background cont.

- In order to protect these elements, the organization must implement controls and protection methods to ensure

  - Access is granted only to the information required; and

  - The use is for the specific reason; and

  - The organization specifically identifies the person

- This requires constant management of access, including additions and removals of privileges, and the logging of their activity, specifically with "super users"

- Common connection method to the organizational network is via remote internet access or connection to the office desktop computer
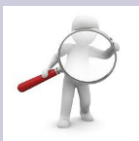
2. Remote Connection- Audit Steps

Connection Via Internet interface

The access can be done via organizational or personal computer (Shadow IT…)

Two phases before granting access- 1. verify an updated anti virus exists; 2. OTP; after these- secured encrypted connection is established

Audit step - disable the anti virus and try to connect

3. Remote Connection to Emails- Background

- As part of the remote workforce practices, employees can get access to their emails and calendar, away from their office desktop computers from several devices

- One of the common devices are cellular handsets

- Email usage has its risks, including
  - Unauthorized email use
  - Virus infection
  - Data leakage

3. Remote Connection to Emails- Audit steps

Filtering and downloading mechanism

Files attached to emails can create a potential risk and contain malicious material
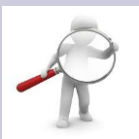
Audit step- examine if there is an effective mechanism to block introducing of dangerous files

4. Equipment and Password used from Remote Access - Background

- This includes several controls and mechanisms

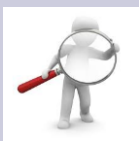| Physical Security and prevention of access	Access and permission	Protection of data

Security software	Security updates

4. Equipment and Password used from Remote Access - Audit steps

Equipment and system hardening

Identification of attacks by viruses and other attacks on the endpoint

Audit step - evaluate the security level and hardening of laptops and devices

Auditing Remote Access Turned Out to Be a Very Effective Engagement

Summary

- Requiring to work from home, of most of the business segment is definitely a game changer that raise many risks

- When COVID-19 will be over, we will most likely fly less, continue to use "Zoom" software and will continue to partially work from home

- Most if not all of the risks described above will continue to be highly relevant to us also in the future and as an Exploitation RM strategy-we can definitely leverage all the experience we have

- Our Audit Approach turned out to be a very effective one and we got positive feedbacks from management and from Audit Committee, I warmly recommend you all to launch it in order to provide an assurance on such an important topic!

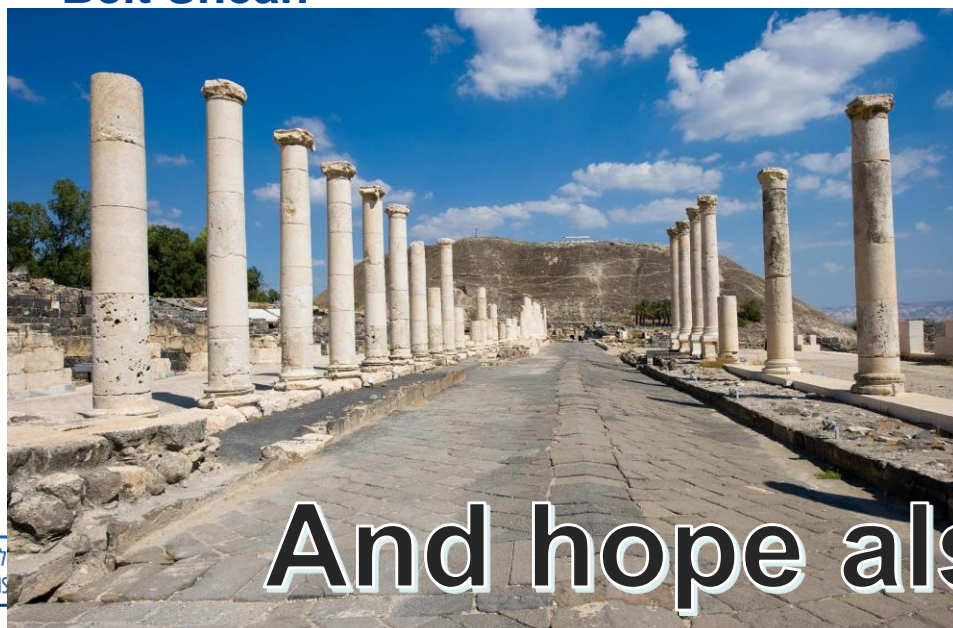# Hope to Meet you in Person Here in Israel!
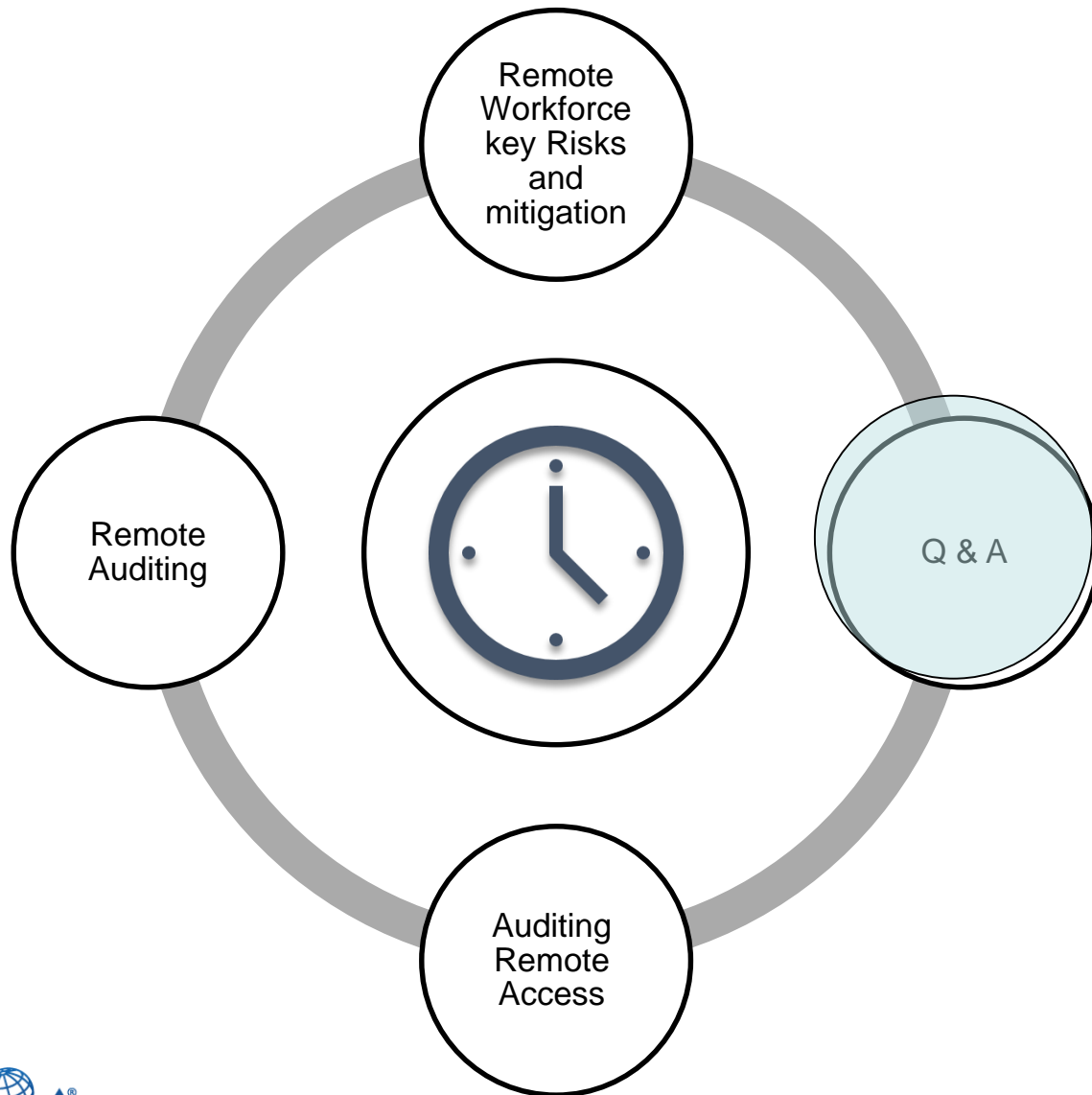
Tel Aviv- Jaffa

Jerusalem

Masada

Beit Shean

The Dead Sea

And hope also in Croatia…

Agenda

Remote Workforce key Risks and mitigation

Remote Auditing

Q & A

Auditing Remote Access

לשכת המבקרים הפנימיים IIA ישראל (חל״צ)
IIA ISRAEL–INSTITUTE OF INTERNAL AUDITORS

Thanks for your Listening!
You are all welcome to keep in touch

✉ Lior.Segal@Gmail.com

📱 +972-50-6773706

in https://www.linkedin.com/in/liorsegal