

Audit of Third Party Service Provider

From an Information Security Perspective

CA. Hemang Doshi
hemangdoshi99@yahoo.co.in

- **Scope of Chartered Accountants in Practice in third party audits**

- **Mandate by most of the regulator like RBI, IRDAI etc.**

IRDAI Mandates:

Internal Audit shall conduct audit for third party /vendors handling critical data on planned and ad hoc basis to measure the effectiveness of the third party security controls implemented

- **Proposed Personal Data Protection Bill**

Clause 29.—This clause seeks to require significant data fiduciaries to have their policies and conduct audited by data auditors.

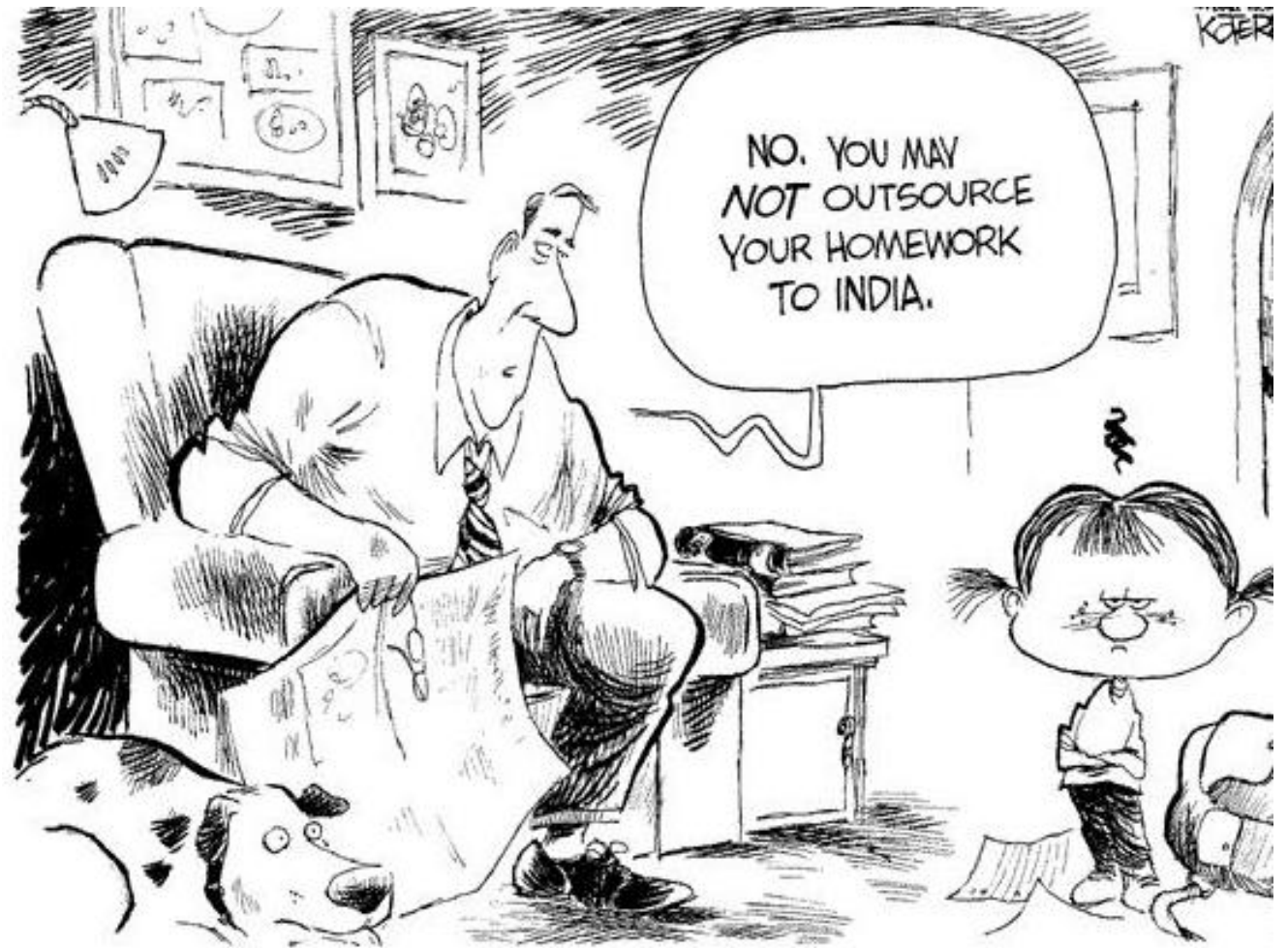
(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.

Third party service provider means a professional body engaged by a organization to provide services to their clients.

Example Includes:

- Call Centre
- BPO
- Date Entry
- TPA

‘Outsourcing of the process’



The Beginning



Auditor should have clear idea about scope and objective of the audit.

Scope of work should be well documented and approved by management.

If audit is mandated by some regulation, auditor should be aware about the underlying requirements.

Example: Awareness about IRDAI checklist for Vendor associated with Insurance Companies. IRDAI mandates for data localization.



Audit Preparation – Essential Factors

Review of Service Level Agreement

Nature of outsourcing, terms of the contract, IS clause, BCP clause etc.

Review last year audit report, if any high risk observations, compliance level

Walkthrough of the process being outsourced
Understand end to end process

Review of risk register of the process/department
understand inherent risk, residual risk and risk appetite

Understand the profile and organization structure of service provider

Private, Partnership, listed, year of existence, employee strength etc.

Must have clauses



*“We have an agreement in principle.
The question is, do we all have the same principles?”*

Service Level Agreement

Right to audit clause

Easy access to service provider’s record, data, documents

Confidentiality clause & Non disclosure agreement

Service provider to obtain NDA from its employees

Information Security Requirements

CIA Triad – Requirements

No outsourcing clause

Most ignored clause

Escrow Arrangement

Applicable for software developers for safe custody of source code

Business Continuity Requirements

Requirements of business continuity during disruption


Audit Checklist – The Magical Document

Audit Checklist should be derived from:

- Service Level Agreement
- Risk Register
- Inputs from the process owner/department/organization
- ISO 27001 controls
- Industry specific requirements

Globally recognized standard for ISMS

As a good practice, checklist should be made available to the service provider in advance.



"Oh yeah, didn't we mention that the audit would include your internet history?"



The Day

Opening Meeting

Introduction – scope-objective – audit plan

Process Walkthrough

Quick understanding of the process

Floor Walkthrough

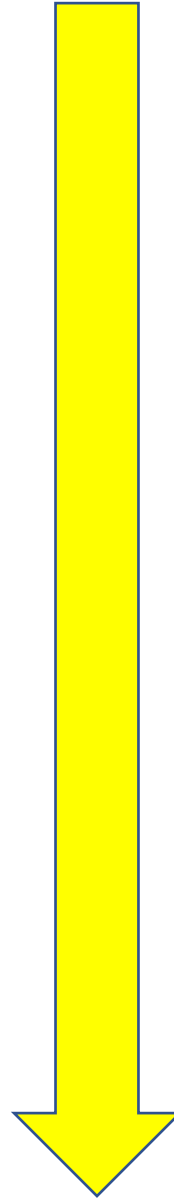
Observe the actual process

Desktop Security

Review the system hardening and control

Run through the audit checklist

Closing Meeting



On the Floor



"I DON'T THINK YOU UNDERSTAND THE CONCEPT OF CYBERSECURITY."

Separate Floor

Exclusive arrangement for organization's process

Understand end to end practice

Input – Process - Output

Data sharing practices

Secured FTP/Encryption/Password Protection

Data purging practices

Use of specialized tools to erase the data

Employee Awareness

Awareness about organization security requirements-
Example Inbound Call Centre

Clear Desk & Clear Screen Policy

No sensitive data on the desk or screen

Desktop Security

Passwords are not pre-saved in browser(s)

Screen saver should be enabled

System date and time – Admin Controls

Guest user account should be disabled

Deployment of password framework

Regedit/System 32/Logs – Admin Controls

Synchronization with Network Time Protocol (NTP)

Installation of only authorized Software



Desktop Security

Updated Antivirus

Windows Firewall and Windows Defender Security

Windows – Patch Update

Browsers – Updated versions

Genuine Operating System



Pre-saved passwords

The image shows a Chrome browser window with the Google homepage. The address bar is empty. The main content area displays the Google logo with a pink heart above the second 'o' and a colorful penguin character on the right. Below the logo is a search bar with the text "Search Google or type a URL". At the bottom of the page, there are three shortcuts: "Google Accou...", "Web Store", and "Add shortcut". A "Customize" button is located in the bottom right corner of the page.

The browser's menu is open on the right side, showing the following options:

- New tab (Ctrl+T)
- New window (Ctrl+N)
- New incognito window (Ctrl+Shift+N)
- History
- Downloads (Ctrl+J)
- Bookmarks
- Zoom: - 100% +
- Print... (Ctrl+P)
- Cast...
- Find... (Ctrl+F)
- More tools
- Edit | Cut | Copy | Paste
- Settings (highlighted with a red arrow)
- Help
- Exit

Pre-saved passwords

Settings

Search settings

You and Google

Autofill

Appearance

Search engine

Default browser

On startup

Advanced

Extensions

About Chrome

Get Google smarts in Chrome

Sync and personalize Chrome across your devices

Turn on sync...

Sync and Google services

Chrome name and picture

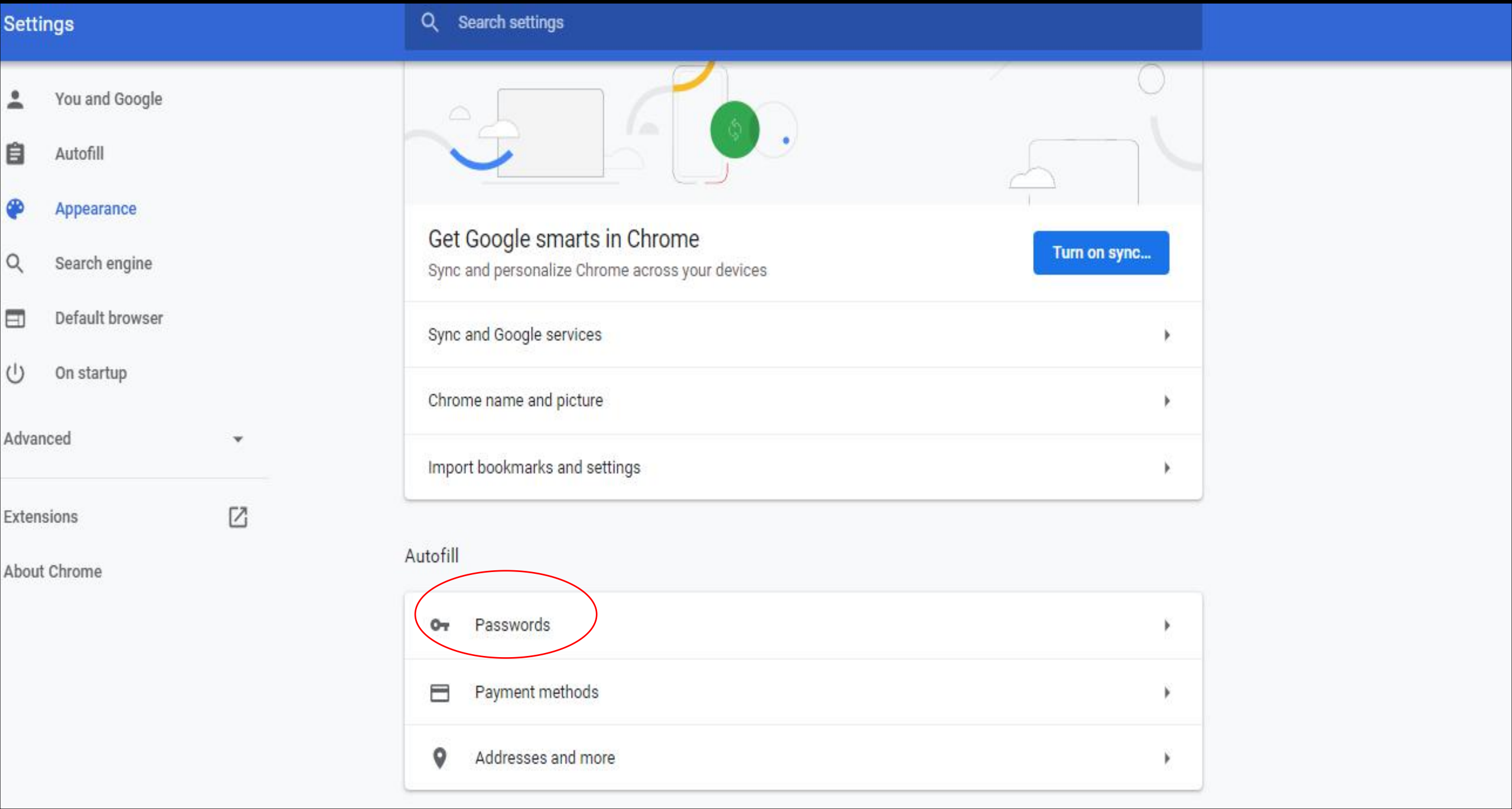
Import bookmarks and settings

Autofill

Passwords

Payment methods

Addresses and more

The image shows the Chrome Settings interface. On the left is a navigation sidebar with categories like 'You and Google', 'Autofill', 'Appearance', 'Search engine', 'Default browser', 'On startup', 'Advanced', 'Extensions', and 'About Chrome'. The main content area is titled 'Get Google smarts in Chrome' and includes a 'Turn on sync...' button and a list of settings: 'Sync and Google services', 'Chrome name and picture', and 'Import bookmarks and settings'. Below this is the 'Autofill' section, which contains three items: 'Passwords', 'Payment methods', and 'Addresses and more'. The 'Passwords' item is circled in red.

Pre-saved passwords

← Passwords



🔍 Search passwords

Offer to save passwords

Auto Sign-in

Automatically sign in to websites using stored credentials. If disabled, you will be asked for confirmation every time before signing in to a website.



High risk if passwords are saved for critical applications

View and manage saved passwords in your [Google Account](#)

Saved Passwords



Website

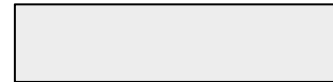
Username

Password



192.168.0.1

Admin



cisaexamstudy.com

hemangdoshi99



Updated Browser

The image shows a screenshot of a web browser window displaying the Google homepage. The browser's address bar shows the URL `https://www.google.com/#spf=1587033202323`. The Google logo is prominently displayed in the center, with a special edition where the letter 'g' is replaced by a chef's hat and a cooking pan, and the letter 'l' is replaced by a stack of brown boxes. Below the logo is a search bar with a magnifying glass icon. Two buttons, "Google Search" and "I'm Feeling Lucky", are positioned below the search bar. A message reads "To all food service workers, thank you". At the bottom, it says "Google offered in: हिन्दी बांग्ला తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ".

A context menu is open on the right side of the browser window, listing various options:

- Print
- File
- Zoom (100%)
- Safety
- Open with Microsoft Edge (Ctrl+Shift+E)
- Add site to Apps
- View downloads (Ctrl+J)
- Manage add-ons
- F12 Developer Tools
- Go to pinned sites
- Compatibility View settings
- Internet options
- About Internet Explorer

A red arrow points from the "About Internet Explorer" option in the context menu to the "To all food service workers, thank you" message on the page.

At the bottom of the browser window, there is a footer with links for "Advertising", "Business", "About", and "How Search works" on the left, and "Privacy", "Terms", and "Settings" on the right. The Windows taskbar is visible at the very bottom, showing the Start button, a search bar, and several application icons.

About Internet Explorer



IE 11 is the latest version

Microsoft do not release patch for earlier versions



Internet Explorer[®]11

Version: 11.973.17763.0

Update Versions: 11.0.170 (KB4534251)

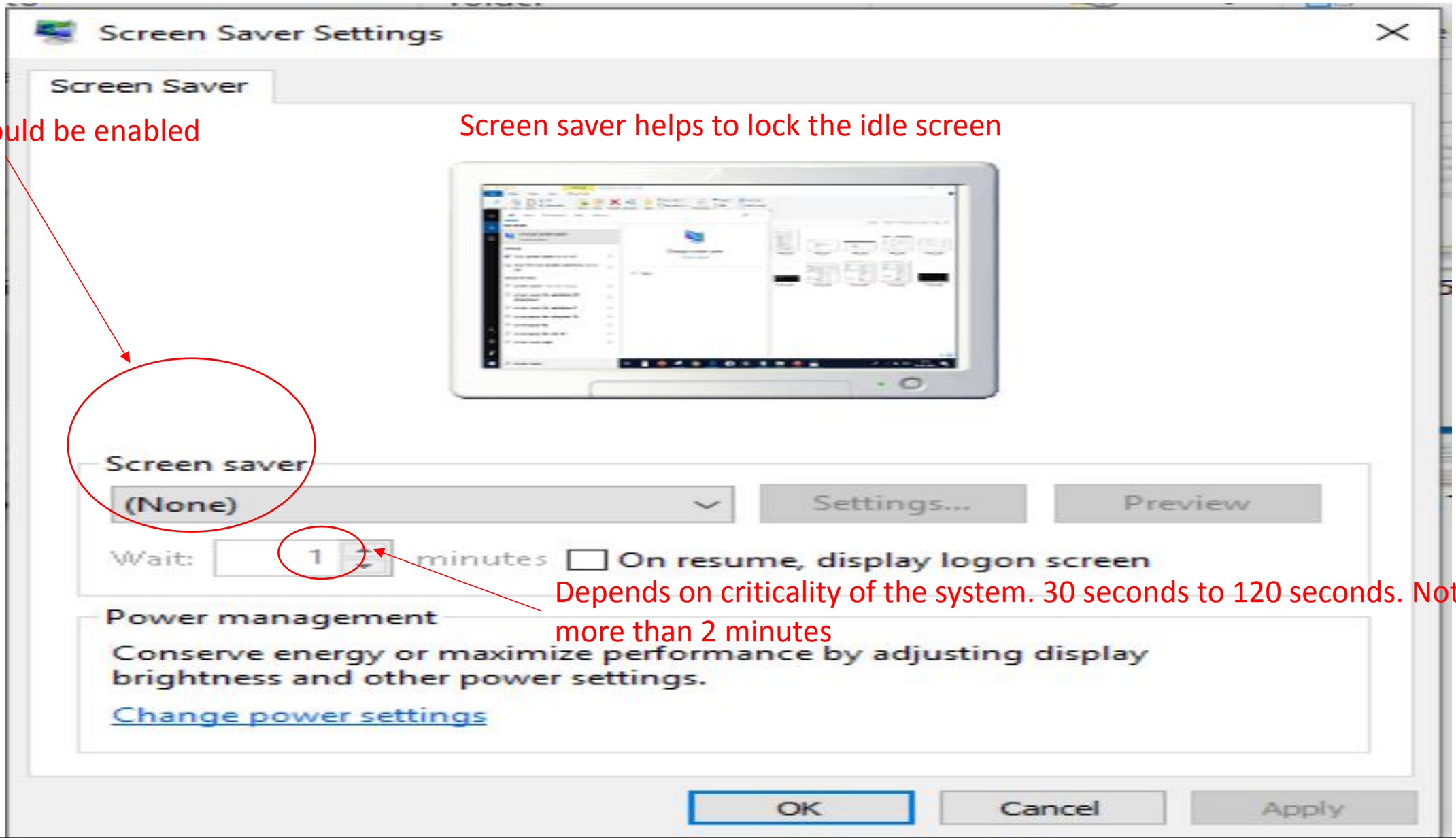
Product ID: 00150-20000-00003-AA459

© 2015 Microsoft Corporation. All rights reserved.

Close

Screen Saver

Search/Run - 'change screen saver'



This should be enabled

Screen saver helps to lock the idle screen

Screen saver

(None)

Settings...

Preview

Wait:

1

minutes

On resume, display logon screen

Power management

Conserve energy or maximize performance by adjusting display brightness and other power settings.

[Change power settings](#)

OK

Cancel

Apply

Depends on criticality of the system. 30 seconds to 120 seconds. Not more than 2 minutes

Window Version

Search/Run - 'winver'



Windows 10 is the latest version

Microsoft do not release patch for earlier versions

Window Version

Search/Run - 'activation'

Apart from compliance issue, unlicensed version is prone to malware attack

Settings

Home

Find a setting

Update & Security

- Windows Update
- Delivery Optimization
- Windows Security
- Backup
- Troubleshoot
- Recovery
- Activation
- Find my device
- For developers
- Windows Insider Program

Activation

Windows

Edition Windows 10 Home Single Language
Activation Windows is activated with a digital license
[Learn more](#)

Upgrade your edition of Windows

Upgrade to Windows 10 Pro to add features that help you connect to company networks, access one PC from another, encrypt your data and more.

Go to the Store to buy the upgrade or enter a product key.

[Go to the Store](#)

[Change product key](#)

Add a Microsoft account

Your Microsoft account unlocks benefits that make your experience with Windows better, including the ability to reactivate Windows 10 on this device.

[Learn more](#)

Where's my product key?

Depending on how you got Windows, activation will use a digital license or a product key.

[Get more info about activation](#)

Have a question?

[Finding your product key](#)

[Get help](#)

[Give feedback](#)

Search/Run - 'virus and threat protection'

Windows Security



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.

Last scan: 30-03-2020 14:20 (quick scan)

0 threats found.

Scan lasted 7 minutes 59 seconds

45721 files scanned.

Quick scan

[Scan options](#)

[Allowed threats](#)

[Protection history](#)

As a good practice, scan should happen every 7 days

Signature should get updated almost on daily basis

Search/Run - 'view update history'

← Settings

View update history

[Uninstall updates](#)

[Recovery options](#)

Update history

▼ Feature Updates (1)

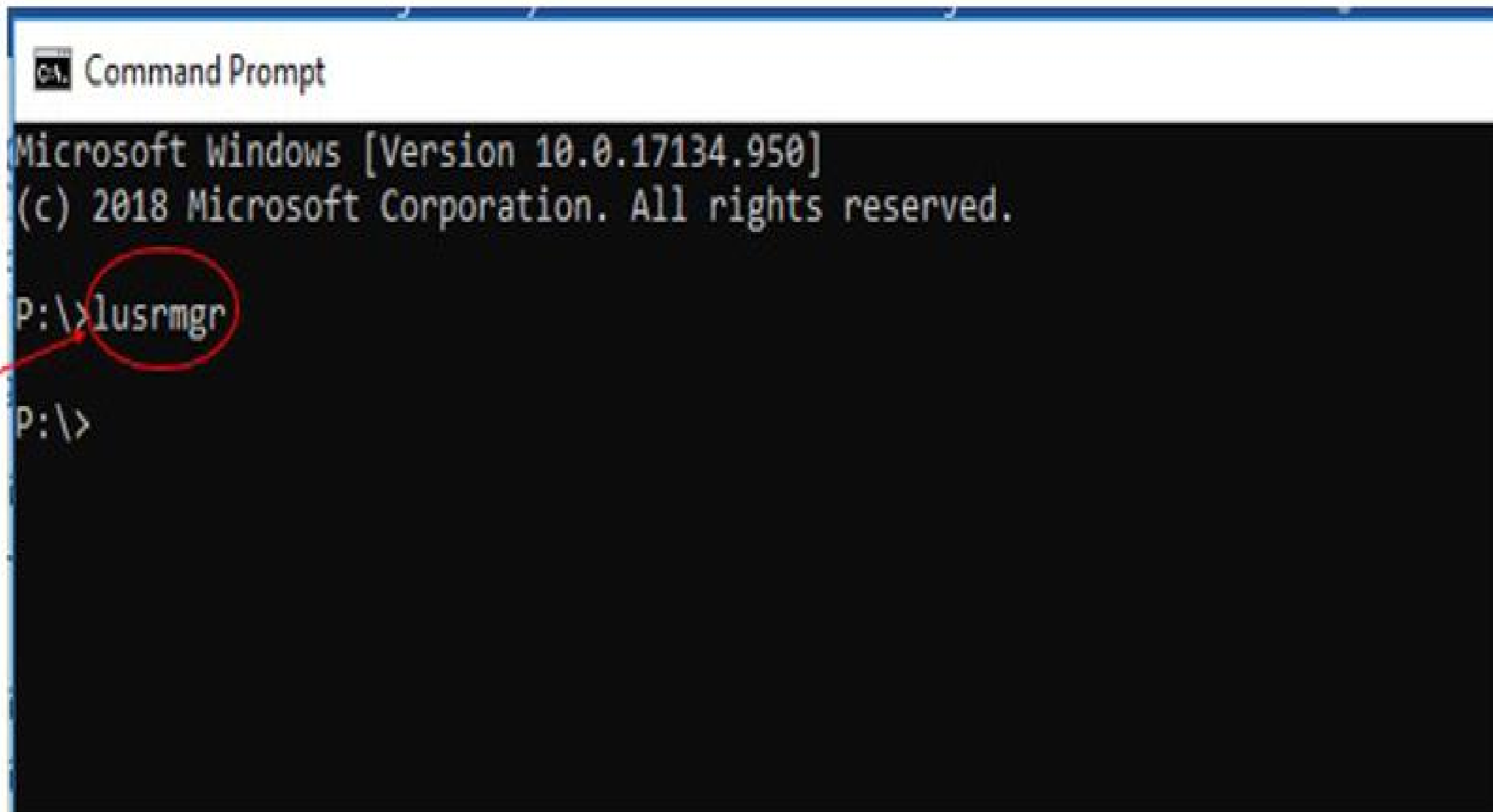
Feature update to Windows 10, version 1909

Successfully installed on 16-04-2020

[See what's new in this update](#)

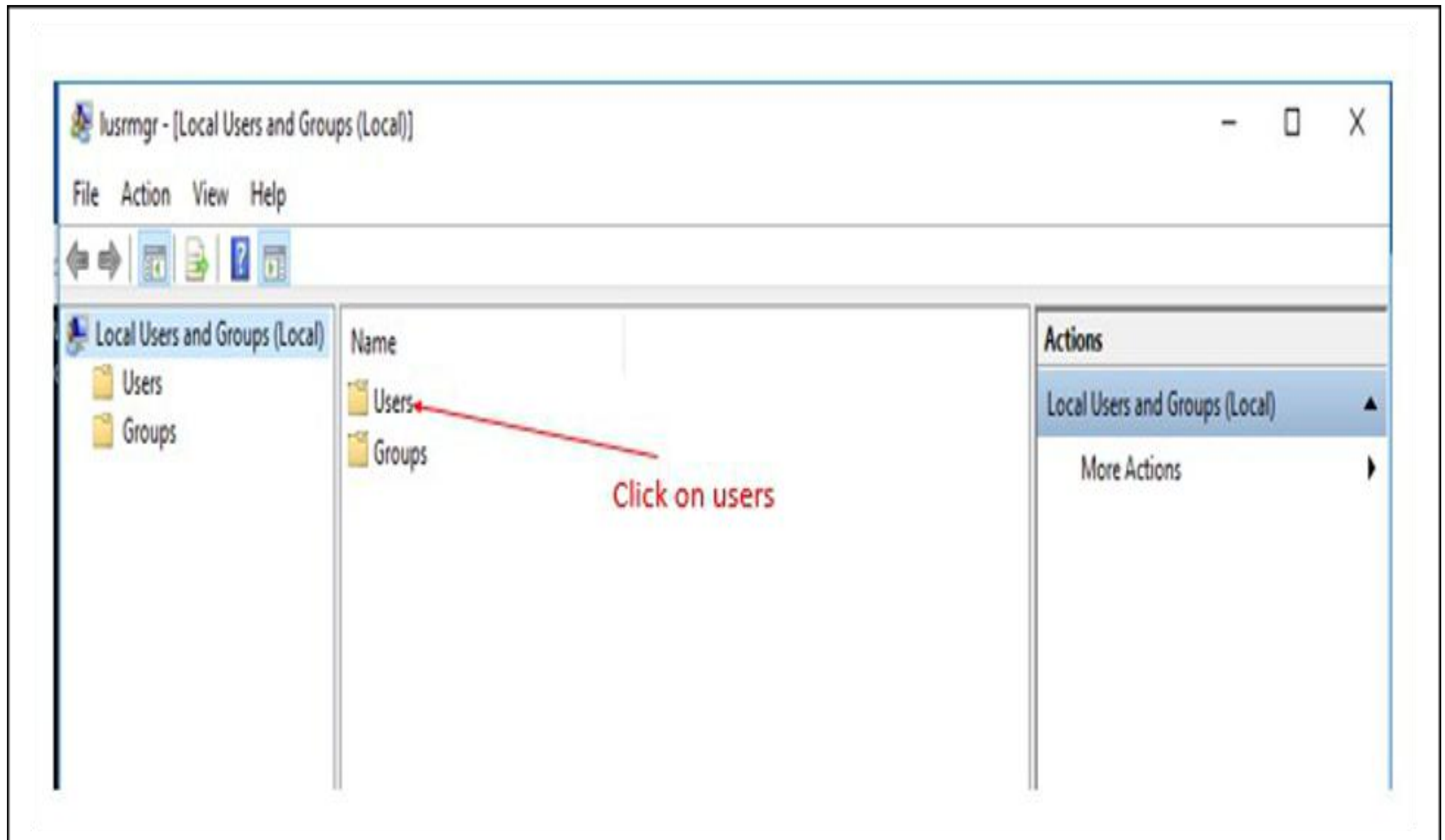
Last update should be within a month

Enter
command -
lusrmgr



```
CA. Command Prompt
Microsoft Windows [Version 10.0.17134.950]
(c) 2018 Microsoft Corporation. All rights reserved.
P:\>lusrmgr
P:\>
```

Guest Users



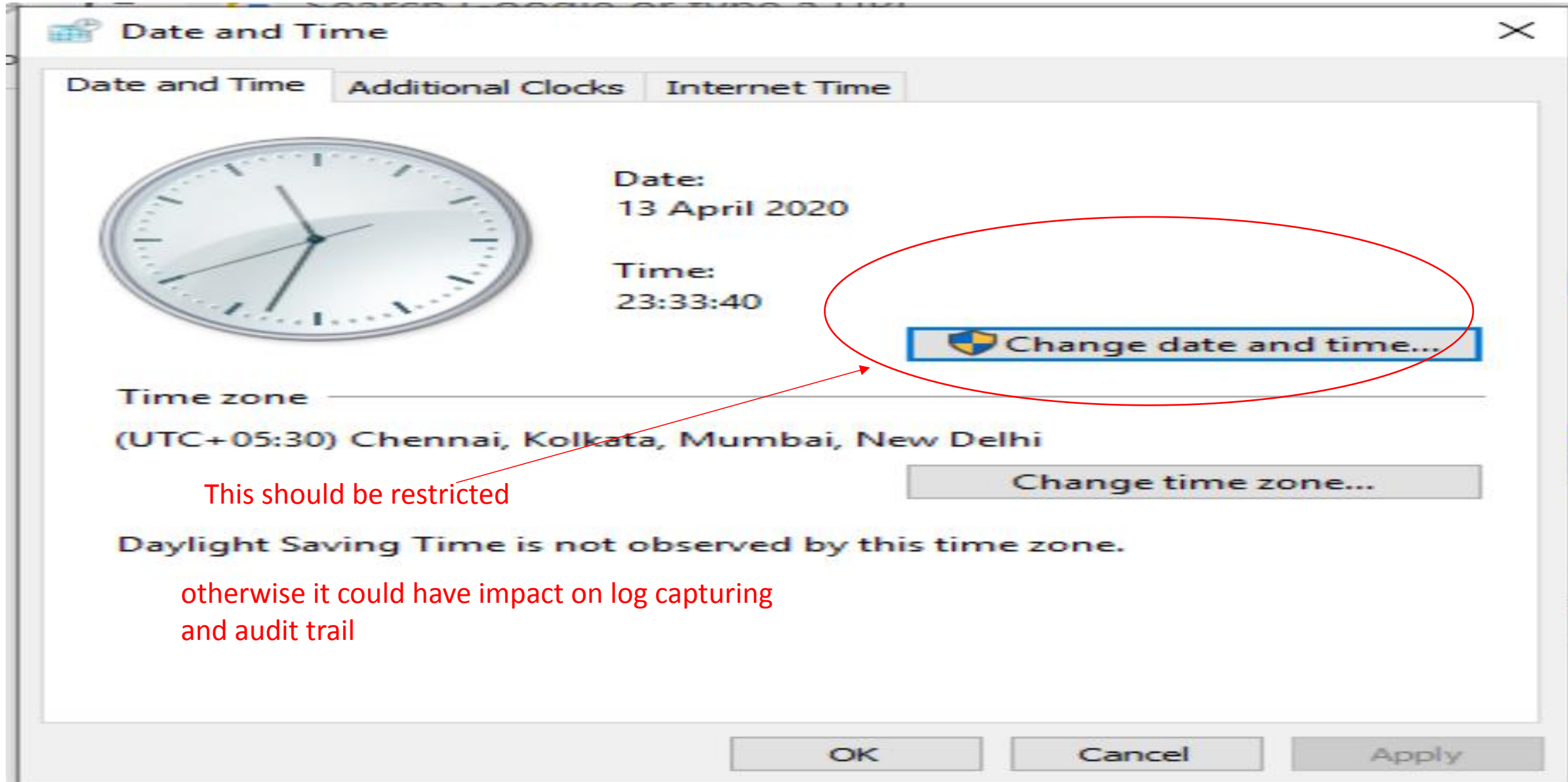
The screenshot shows the Windows Computer Management console. The left-hand navigation pane is expanded to 'Local Users and Groups' > 'Users'. The main pane displays a list of users with columns for Name, Full Name, and Description. The 'Guest' user is highlighted with a red circle, and a red arrow points from a text box to the down arrow in its user icon.

Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
Guest		Built-in account for guest access t...

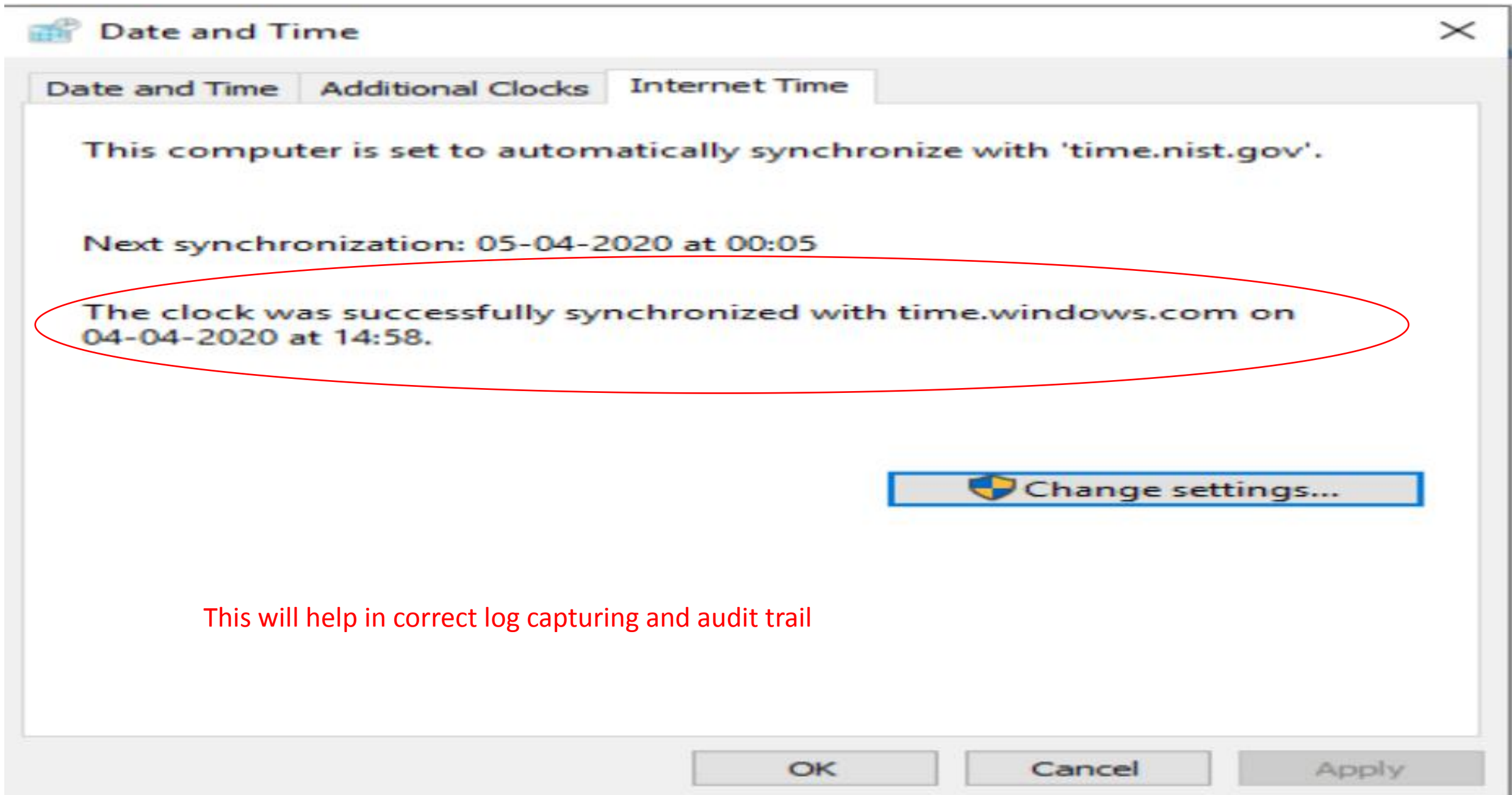
Down arrow in the logo indicates that account is disabled

Change Date & Time

Search/Run - 'change date and time'



Clock Synchronization



This will help in correct log capturing and audit trail

Reviewing the installed software

Programs and Features

Control Panel > Programs > Programs and Features

Control Panel Home

Uninstall or change a program

View installed updates

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair

Turn Windows features on or off

Organize

Name	Publisher	Installed On	Size	Version
AccessData FTK Imager	AccessData	15-12-2019	77.6 MB	3.1.3.2
Active Whois 3.2	Ivan Mayrakov	14-12-2019		3.1
Adobe Digital Editions 4.5	Adobe Systems Incorporated	06-08-2019	20.7 MB	4.5.10
Adobe Reader XI (11.0.23)	Adobe Systems Incorporated	04-12-2018	313 MB	11.0.23
airtel	Huawei Technologies Co.,Ltd	14-12-2019		23.015.02.14.284
Autopsy	The Sleuth Kit	15-12-2019	537 MB	3.1.3
Cisco WebEx Meetings	Cisco WebEx LLC	15-12-2018		
Dell Digital Delivery	Dell Products, LP	03-08-2019	2.45 MB	3.5.2013.0
Dell Help & Support	Dell Inc.	09-04-2019	58.4 MB	2.6.1.0
Dell SupportAssist	Dell Inc.	21-03-2020	180 MB	3.4.5.366
Dell SupportAssist Remediation	Dell Inc.	15-12-2018	22.1 MB	4.1.0.6828
Dell Touchpad	Synaptics Incorporated	22-05-2019	46.4 MB	19.2.17.70
Dell Update	Dell Inc.	27-03-2020	29.5 MB	3.1.1
Dell Update - SupportAssist Update Plugin	Dell Inc.	09-04-2019	11.5 MB	4.1.0.6828
eMailTrackerPro		14-12-2019		
Event Log Explorer 3.3	FSPro Labs	15-12-2019	6.54 MB	3.3
Free Photo Viewer	10-Strike Software	05-12-2017	2.93 MB	1.3
Google Chrome	Google LLC	11-04-2020	353 MB	80.0.3987.163
Grammarly for Microsoft® Office Suite	Grammarly	27-12-2018	23.6 MB	6.7.154
IDEA 10.2	CaseWare IDEA Inc	22-11-2019	376 MB	10.2.1.56
Intel(R) Dynamic Platform and Thermal Framework	Intel Corporation	15-12-2018	26.7 MB	8.3.10207.5567
Intel(R) HID Event Filter	Intel Corporation	22-05-2019	3.00 MB	2.2.1.372
Intel(R) Wireless Bluetooth(R)	Intel Corporation	16-07-2017	17.6 MB	19.01.1627.3533
Intel® Graphics Driver	Intel Corporation	15-12-2018	74.2 MB	23.20.16.4973
Intel® Management Engine Components	Intel Corporation	22-05-2019	97.1 MB	1846.12.0.1177

Currently installed programs Total size: 4.65 GB
61 programs installed

Compare this with approved software list

Unauthorized software should be reported



"Why do we have to change our passwords?
It's not like anyone could ever guess it"

Password Management

Password Complexity

Capital letter – special character – min 8 character etc.

Sharing of first time password

Should be made available to the user only

Maximum Password Age

Automatic expiry of the password at defined interval

Single Sign On

Risk of single point of failure

Password Deployment

CMD – type command 'net accounts'

Command Prompt

```
Microsoft Windows [Version 10.0.17763.973]  
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\> net accounts  
Force user logoff how long after time expires?:  
Minimum password age (days):  
Maximum password age (days):  
Minimum password length:  
Length of password history maintained:  
Lockout threshold:  
Lockout duration (minutes):  
Lockout observation window (minutes):  
Computer role:  
The command completed successfully.
```

Enter the command 'net accounts'

Never
0
42
0
None
Never
30
30
WORKSTATION

Compare these variables with password policy

Report the deviation

Asset Management



Inventory of Assets

desktop, laptop, servers, network device etc.

Ownership of Assets

owner is responsible for the safeguard of the data.

Classification of Assets

critical , non critical etc. Stringent controls for critical assets.

HR Aspects

Recruitment Process

interview structure, background verification process

Induction Process

coverage of information security training

Providing various Access

need to know basis, appropriate approvals

Training Process

information security training at frequent interval

Defined Job Descriptions

documented roles and responsibilities

Exit Process

termination of all accesses immediately



"Until we implement a complete segregation of duties solution the auditor said we will need to press the 'enter' key together"

Network Security



"Can you make the penetration testing stop?
I think we've been penetrated enough!"

Placement & Control of firewall

network diagram, firewall controls, approval for rule changes

Log Monitoring

log capturing and monitoring process

Deny All or Allow All

traffic rules for critical system, appropriate approvals

ISP Redundancy

network backup

Data Sharing - SFTP

VAPT Process

VAPT process, frequency and compliance level



Email Security

Control on Shared Email ID

only unique email IDs, approval for shared email IDs, appropriate controls

Anti-Virus scanning for attachments

Encryption/Password Protection for Data Sharing

Domain based Email Restrictions

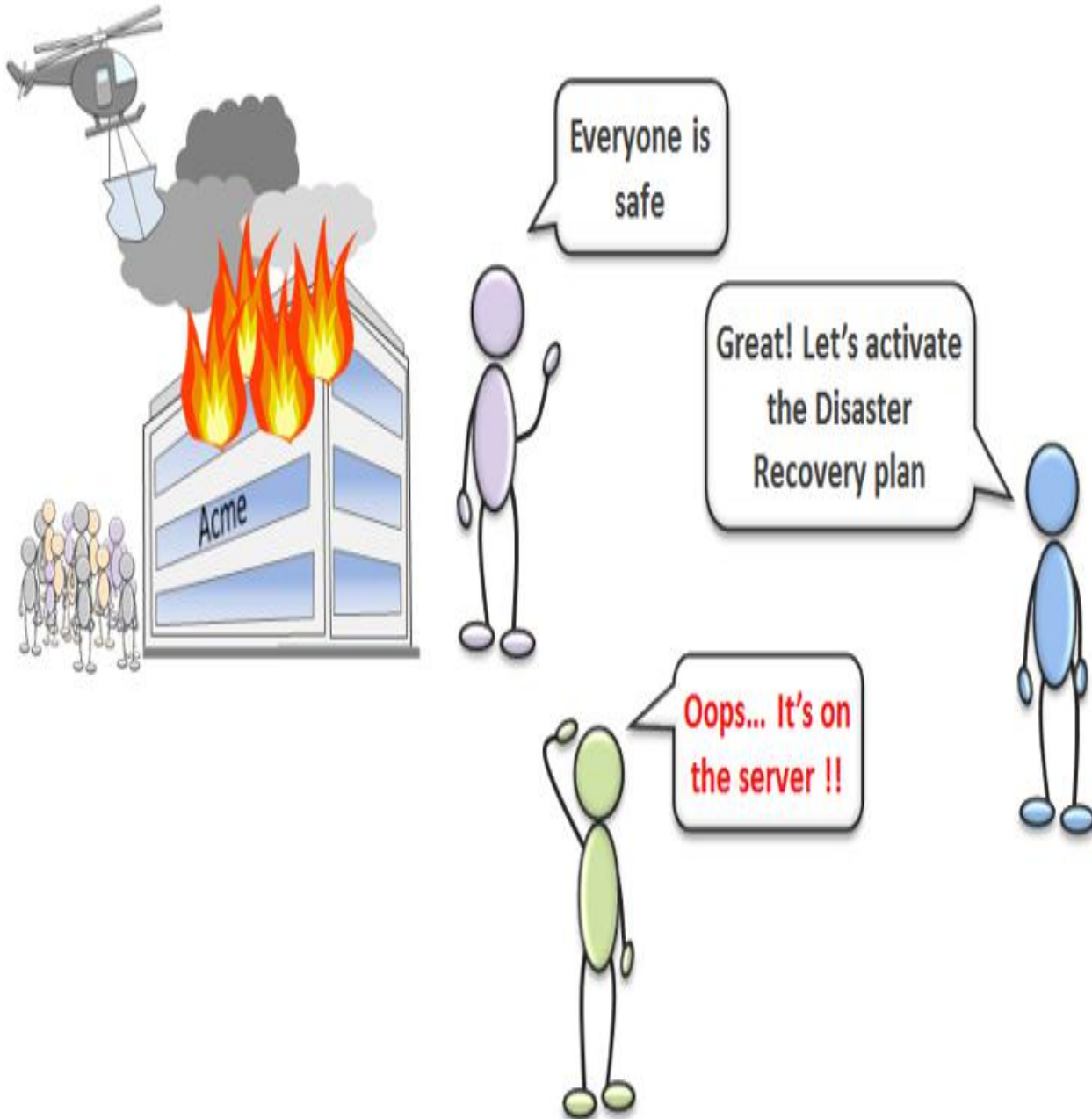
email communication with only approved domains

Email Retention

Email Backup

Approved Email Usage Policy

Business Continuity Arrangements



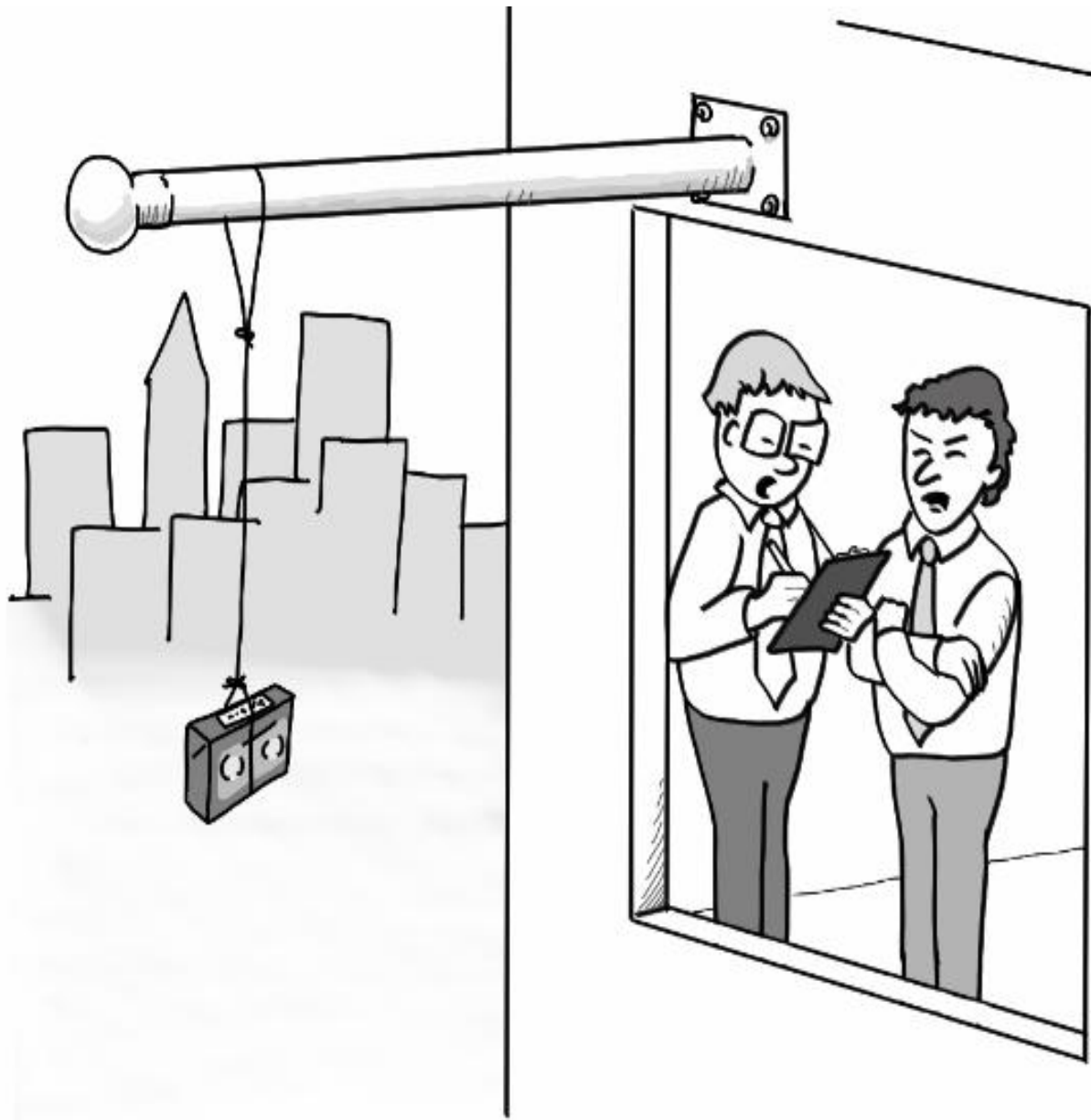
Availability of approved BCP & DRP
approved documents, version controls

Periodic Review

BCP Testing

frequency, test results and analysis

BCP Training



"This is not technically off-site storage"
"What, do I need a longer pole?"

Backup Management

Availability of approved backup policy
approved documents, version controls

Restoration Test

frequency, test results and analysis

Backup Media Management

security

Offsite Storage of the Backup

different seismic zone

Compliance & Risk Management

Risk Management Procedure

Compliance Procedure

Internal Audit Procedure



Policies & Procedures

Availability of documented policies and procedures

Annual review and updation

Approval Process

Version Control

Adequacy of the policy

Awareness amongst the staff



"It says 'please wait while critical updates are installed'"



17-factor authentication

Logical Access Controls

Authorization Process

Authentication Process

Two factor of authentication

Privilege Access

Need to Know

Generic Accounts

Log capturing & Monitoring

User Access Review

Closing Meeting

Discuss findings

Obtain auditee's view

Discuss recommendation and closure timeline

Take sign off



“Well I think you should tell him about the discrepancies we found.”



I think now you will also agree that our report do carry weight

Audit Report

It is important to determine that whether audit report has created any added value for the client

Thank You