Checklist

Google chrome

1.1.1 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Enabled'

1.1.2 (L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled'

1.1.3 (L1) Ensure 'Always runs plugins that require authorization' is set to 'Disabled'

1.1.4 (L1) Ensure 'Block third party cookies' is set to 'Enabled'

1.1.5 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled'

1.1.6 (L1) Ensure 'Enable AutoFill' is set to 'Disabled'

1.1.7 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled'

1.1.8 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled'

1.1.9 (L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled'

1.1.10 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled'

1.1.11 (L1) Ensure 'Specify whether the plugin finder should be disabled' is set to 'Enabled'

1.2 Allow Google Chrome Frame to Handle the Following Content Types

1.3.1 (L1) Ensure 'Configure the required domain name for remote access hosts' is set to 'Enabled'

1.3.2 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled'

1.3.3 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled'

1.3.4 (L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled'

1.4.1 (L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session)

1.4.2 (L1) Ensure 'Default Plugin Setting' is set to 'Enabled' (Click to Play)

1.5 Default HTML Renderer for Google Chrome Frame

1.6 Default Search Provider

1.7 Extensions

1.7.1 (L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("*" for all extensions)

1.8 Home Page

1.9 Locally Managed Users Settings

1.10 Native Messaging

1.11 Password Manager

1.11.1 (L1) Ensure 'Enable the password manager' is set to 'Disabled'

1.12 Policies for HTTP Authentication

1.13 Proxy Server

1.14 Startup Pages

1.1.1 (L2) Ensure 'Allow invocation of file selection dialogs' is set to 'Enabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowFileSelectionDialogs
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Allow invocation of file selection
dialogs
```

1.1.2 (L1) Ensure 'Allow running plugins that are outdated' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AllowOutdatedPlugins
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Allow running plugins that are outdated
```

1.1.3 (L1) Ensure 'Always runs plugins that require authorization' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AlwaysAuthorizePlugins
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Always runs plugins that require
authorization
```

1.1.4 (L1) Ensure 'Block third party cookies' is set to 'Enabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BlockThirdPartyCookies
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Block third party cookies
```

1.1.5 (L1) Ensure 'Continue running background apps when Google Chrome is closed' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:BackgroundModeEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Continue running background apps when
Google Chrome is closed
```

1.1.6 (L1) Ensure 'Enable AutoFill' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:AutoFillEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Enable AutoFill
```

1.1.7 (L1) Ensure 'Enable Google Cloud Print Proxy' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CloudPrintProxyEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Enable Google Cloud Print Proxy
```

1.1.8 (L1) Ensure 'Enable reporting of usage and crash-related data' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:MetricsReportingEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Enable reporting of usage and
crash-related data
```

1.1.9 (L1) Ensure 'Enable submission of documents to Google Cloud print' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:CloudPrintSubmitEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Enable submission of documents to Google
Cloud print
```

1.1.10 (L1) Ensure 'Import saved passwords from default browser on first run' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:ImportSavedPasswords`

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Import saved passwords from default
browser on first run
```

1.1.11 (L1) Ensure 'Specify whether the plugin finder should be disabled' is set to 'Enabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DisablePluginFinder`

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Specify whether the plugin finder should
be disabled
```

1.3.1 (L1) Ensure 'Configure the required domain name for remote access hosts' is set to 'Enabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostDomain`

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` and enter domain.

```
Computer Configuration\Administrative Templates\Classic Administrative
Templates (ADM)\Google\Google Chrome\Configure remote access
options\Configure the required domain name for remote access hosts
```

1.3.2 (L1) Ensure 'Enable curtaining of remote access hosts' is set to 'Enabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostRequireCurtain
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Templates (ADM)\Google\Google Chrome\Configure remote access options\Enable
curtaining of remote access hosts
```

1.3.3 (L1) Ensure 'Enable firewall traversal from remote access host' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostFirewallTraversal
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Configure remote access options\Enable
firewall traversal from remote access host
```

1.3.4 (L1) Ensure 'Enable or disable PIN-less authentication for remote access hosts' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:RemoteAccessHostAllowClientPairing
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to ``Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Templates (ADM)\Google\Google Chrome\Configure remote access options\Enable
or disable PIN-less authentication
```

1.4.1 (L2) Ensure 'Default cookies setting' is set to 'Enabled' (Keep cookies for the duration of the session)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultCookiesSetting
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Content Settings\Default cookies setting
```

1.4.2 (L1) Ensure 'Default Plugin Setting' is set to 'Enabled' (Click to Play)

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:DefaultPluginsSetting
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`with click to play selected from the drop down.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Content Settings\Default Plugins Setting
```

1.7.1 (L1) Ensure 'Configure extension installation blacklist' is set to 'Enabled' ("" for all extensions)*

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallBlacklist\1
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Extensions\Configure Extension
Installation Blacklist
```

1.11.1 (L1) Ensure 'Enable the password manager' is set to 'Disabled'

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome:PasswordManagerEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Disabled.

```
Computer Configuration\Administrative Templates\Classic Administrative
Template (ADM)\Google\Google Chrome\Password manager\Enable the password
manager
```