



ASSESSOR'S PLAYBOOK INSTRUCTIONS



- The Assessor's Playbook is an editable document and an organized way of providing artifacts to your assessor to help expedite your assessment. The Playbook is arranged with the CMMC Level 2 controls

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)

Thursday, July 15, 2021 5:34 PM

- AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices
- AC.L1-3.1.2: Limit information system access to the types of transactions and functions that authorized users are permitted to perform
- AC.L1-3.1.20: Verify and control/limit connections to and use of external information systems
- AC.L1-3.1.22: Control information posted or processed on publicly accessible information systems
- AC.L2-3.1.3: Control the flow of CUI in accordance with approved authorizations
- AC.L2-3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion
- AC.L2-3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts
- AC.L2-3.1.6: Use non-privileged accounts or roles when accessing non-security functions
- AC.L2-3.1.7: Prevent non-privileged users from executing privileged functions and capture the execution of such functions
- AC.L2-3.1.8: Limit unsuccessful logon attempts
- AC.L2-3.1.9: Provide privacy and security notices consistent with applicable CUI rules
- AC.L2-3.1.10: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity
- AC.L2-3.1.11: Terminate (automatically) user sessions after a defined condition
- AC.L2-3.1.12: Monitor and control remote access sessions
- AC.L2-3.1.13: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions
- AC.L2-3.1.14: Route remote access via managed access control points
- AC.L2-3.1.15: Authorize remote execution of privileged commands and remote access to security-relevant information
- AC.L2-3.1.16: Authorized wireless access prior to allowing such connections
- AC.L2-3.1.17: Protect wireless access using authentication and encryption
- AC.L2-3.1.18: Control connection of mobile devices
- AC.L2-3.1.19: Encrypt CUI on mobile devices and mobile computing platforms
- AC.L2-3.1.21: Limit use of portable storage devices on external systems

- First, highlight the control you want to populate with your artifacts on the right pane.

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices

AC.L1-3.1.2: Limit information system access to the types of transactions and functions that authorized users are permitted to perform

AC.L1-3.1.20: Verify and control/limit connections to and use of external information systems

AC.L1-3.1.22: Control information posted or processed on publicly accessible information systems

AC.L2-3.1.3: Control the flow of CUI in accordance with approved authorizations

AC.L2-3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion

AC.L2-3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts

AC.L2-3.1.6: Use non-privileged accounts or roles when accessing non-security functions

AC.L2-3.1.7: Prevent non-privileged users from executing privileged functions and capture the execution of such functions

AC.L2-3.1.8: Limit unsuccessful logon attempts

AC.L2-3.1.9: Provide privacy and security notices consistent with applicable CUI rules

AC.L2-3.1.10: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity

AC.L2-3.1.11: Terminate (automatically) user sessions after a defined condition

AC.L2-3.1.12: Monitor and control remote access sessions

AC.L2-3.1.13: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions

AC.L2-3.1.14: Route remote access via managed access control points

AC.L2-3.1.15: Authorize remote execution of privileged commands and remote access to security-relevant information

AC.L2-3.1.16: Authorized wireless access prior to allowing such connections

AC.L2-3.1.17: Protect wireless access using authentication and encryption

AC.L2-3.1.18: Control connection of mobile devices

AC.L2-3.1.19: Encrypt CUI on mobile devices and mobile computing platforms

AC.L2-3.1.21: Limit use of portable storage devices on external systems

- Next, click the “Insert” ribbon

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)

Thursday, July 15, 2021 5:34 PM

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices

AC.L1-3.1.2: Limit information system access to the types of transactions and functions that authorized users are permitted to perform

AC.L1-3.1.20: Verify and control/limit connections to and use of external information systems

AC.L1-3.1.22: Control information posted or processed on publicly accessible information systems

AC.L2-3.1.3: Control the flow of CUI in accordance with approved authorizations

AC.L2-3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion

AC.L2-3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts

AC.L2-3.1.6: Use non-privileged accounts or roles when accessing non-security functions

AC.L2-3.1.7: Prevent non-privileged users from executing privileged functions and capture the execution of such functions

AC.L2-3.1.8: Limit unsuccessful logon attempts

AC.L2-3.1.9: Provide privacy and security notices consistent with applicable CUI rules

AC.L2-3.1.10: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity

AC.L2-3.1.11: Terminate (automatically) user sessions after a defined condition

AC.L2-3.1.12: Monitor and control remote access sessions

AC.L2-3.1.13: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions

AC.L2-3.1.14: Route remote access via managed access control points

AC.L2-3.1.15: Authorize remote execution of privileged commands and remote access to security-relevant information

AC.L2-3.1.16: Authorized wireless access prior to allowing such connections

AC.L2-3.1.17: Protect wireless access using authentication and encryption

AC.L2-3.1.18: Control connection of mobile devices

AC.L2-3.1.19: Encrypt CUI on mobile devices and mobile computing platforms

AC.L2-3.1.21: Limit use of portable storage devices on external systems

- Lastly, click “Pictures” and navigate to your screenshot artifact to add it to the document.

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)

Thursday, July 15, 2021 5:34 PM

ACME COMPANY

Employee Onboarding Checklist

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices

AC.L1-3.1.2: Limit information system access to the types of transactions and functions that authorized users are permitted to perform

AC.L1-3.1.20: Verify and control/limit connections to and use of external information systems

AC.L1-3.1.22: Control information posted or processed on publicly accessible information systems

AC.L2-3.1.3: Control the flow of CUI in accordance with approved authorizations

AC.L2-3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion

AC.L2-3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts

AC.L2-3.1.6: Use non-privileged accounts or roles when accessing non-security functions

AC.L2-3.1.7: Prevent non-privileged users from executing privileged functions and capture the execution of such functions

AC.L2-3.1.8: Limit unsuccessful logon attempts

AC.L2-3.1.9: Provide privacy and security notices consistent with applicable CUI rules

AC.L2-3.1.10: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity

AC.L2-3.1.11: Terminate (automatically) user sessions after a defined condition

AC.L2-3.1.12: Monitor and control remote access sessions

AC.L2-3.1.13: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions

AC.L2-3.1.14: Route remote access via managed access control points

AC.L2-3.1.15: Authorize remote execution of privileged commands and remote access to security-relevant information

AC.L2-3.1.16: Authorized wireless access prior to allowing such connections

AC.L2-3.1.17: Protect wireless access using authentication and encryption

AC.L2-3.1.18: Control connection of mobile devices

AC.L2-3.1.19: Encrypt CUI on mobile devices and mobile computing platforms

AC.L2-3.1.21: Limit use of portable storage devices on external systems

- To add more items for the same control, hover over the control until you see a (+) sign and click to add another row.

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)

Thursday, July 15, 2021 5:34 PM

ACME COMPANY

Employee Onboarding Checklist

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices

AC.L1-3.1.2: Limit information system access to the types of transactions and functions that authorized users are permitted to perform

AC.L1-3.1.20: Verify and control/limit connections to and use of external information systems

AC.L1-3.1.22: Control information posted or processed on publicly accessible information systems

AC.L2-3.1.3: Control the flow of CUI in accordance with approved authorizations

AC.L2-3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion

AC.L2-3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts

AC.L2-3.1.6: Use non-privileged accounts or roles when accessing non-security functions

AC.L2-3.1.7: Prevent non-privileged users from executing privileged functions and capture the execution of such functions

AC.L2-3.1.8: Limit unsuccessful logon attempts

AC.L2-3.1.9: Provide privacy and security notices consistent with applicable CUI rules

AC.L2-3.1.10: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity

AC.L2-3.1.11: Terminate (automatically) user sessions after a defined condition

AC.L2-3.1.12: Monitor and control remote access sessions

AC.L2-3.1.13: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions

AC.L2-3.1.14: Route remote access via managed access control points

AC.L2-3.1.15: Authorize remote execution of privileged commands and remote access to security-relevant information

AC.L2-3.1.16: Authorized wireless access prior to allowing such connections

AC.L2-3.1.17: Protect wireless access using authentication and encryption

AC.L2-3.1.18: Control connection of mobile devices

AC.L2-3.1.19: Encrypt CUI on mobile devices and mobile computing platforms

AC.L2-3.1.21: Limit use of portable storage devices on external systems

- Once you've completed adding all your artifacts, you can send the OneNote document to your assessor by clicking on "File" and then selecting "Export".

AC.L1-3.1.1: Limit information system access to au - OneNote

Export

1. Export Current:

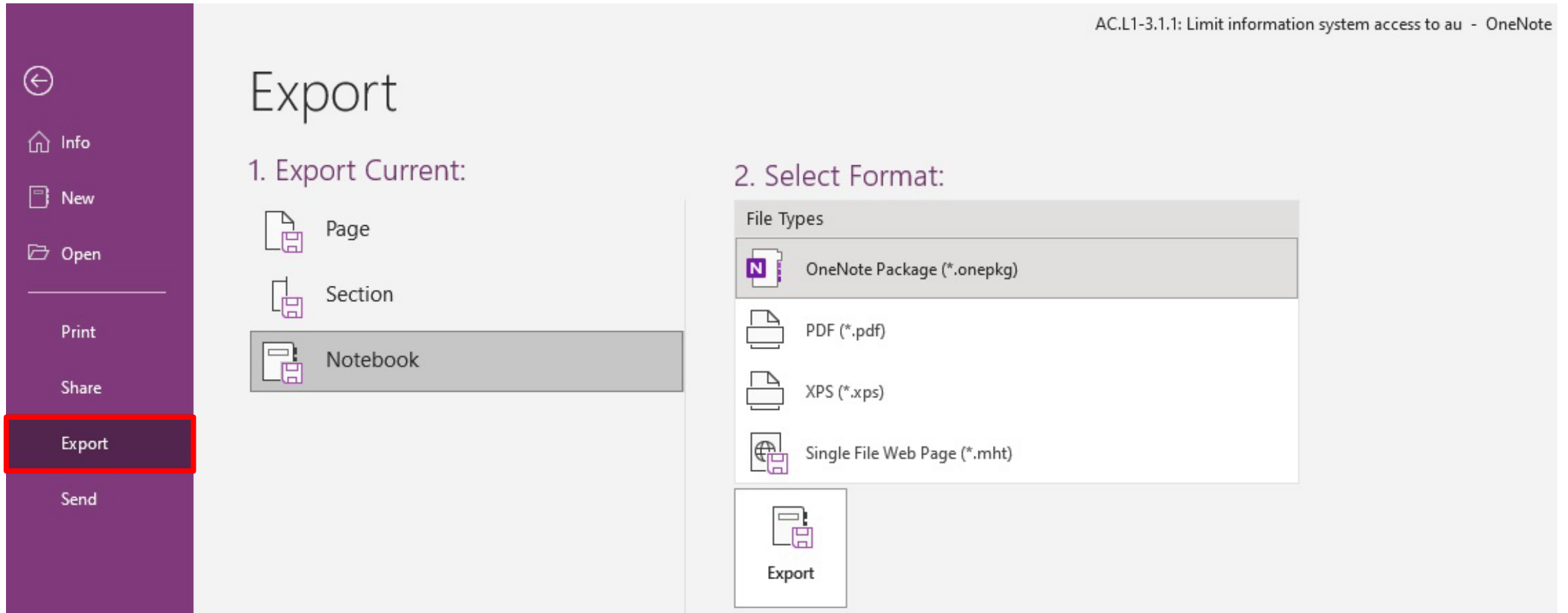
- Page
- Section
- Notebook**

2. Select Format:

File Types

- OneNote Package (*.onepkg)**
- PDF (*.pdf)
- XPS (*.xps)
- Single File Web Page (*.mht)

Export



- Next, select “Notebook”.

AC.L1-3.1.1: Limit information system access to au - OneNote

Export

1. Export Current:

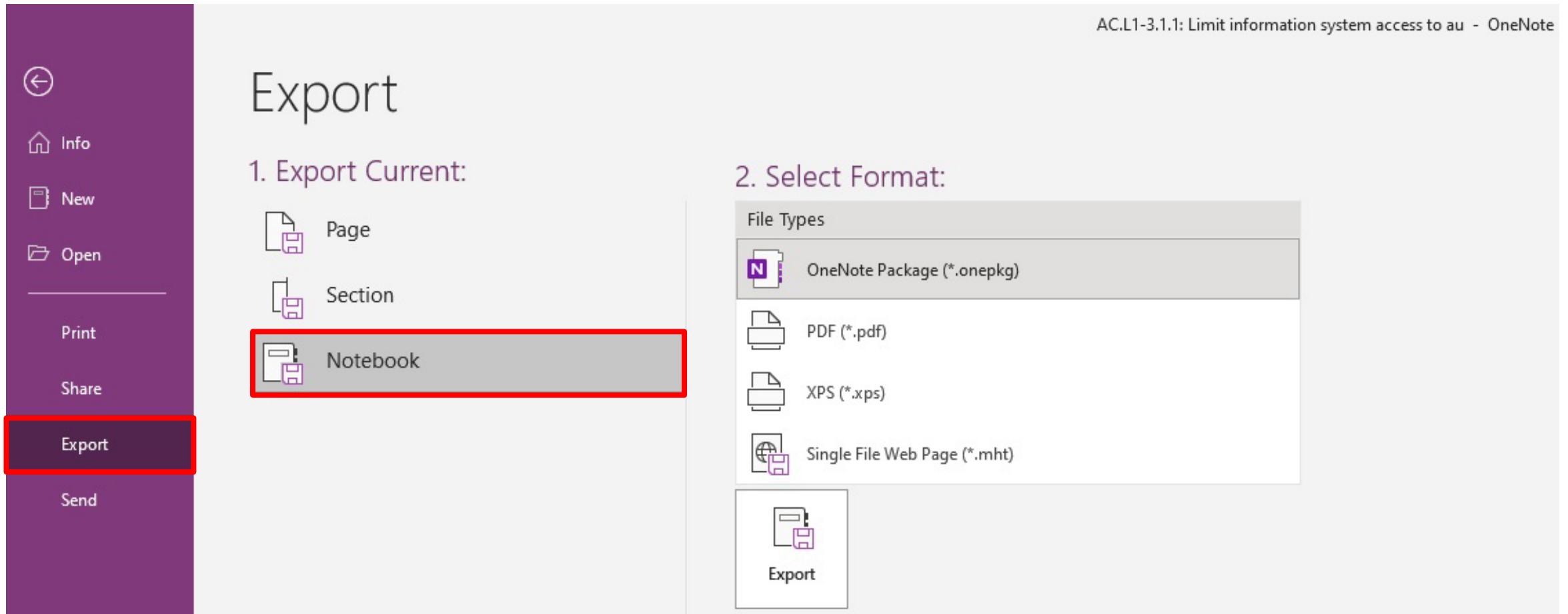
- Page
- Section
- Notebook**

2. Select Format:

File Types

- OneNote Package (*.onepkg)**
- PDF (*.pdf)
- XPS (*.xps)
- Single File Web Page (*.mht)

Export



- Select “OneNote Package (*.onepkg)”.

AC.L1-3.1.1: Limit information system access to au - OneNote

Export

1. Export Current:

- Page
- Section
- Notebook**

2. Select Format:

File Types

- OneNote Package (*.onepkg)**
- PDF (*.pdf)
- XPS (*.xps)
- Single File Web Page (*.mht)

Export

- Lastly, select “Export”.
- Note: The package can exceed 99MB. It’s recommended to utilize a file sharing solution.

AC.L1-3.1.1: Limit information system access to au - OneNote

Export

1. Export Current:

- Page
- Section
- Notebook**

2. Select Format:

File Types

- OneNote Package (*.onepkg)**
- PDF (*.pdf)
- XPS (*.xps)
- Single File Web Page (*.mht)

Export