Home User Security Control Survey

1. Consent Statement for Exempt Research

Title of Study: Using Multi Criteria Decision Making for Security Control Selection in Risk Management Framework
IRB #:
Principal Investigator Name: Dr. Thomas Mazzuchi
Version Date: December 18, 2015

1.

You are invited to participate in a research study under the direction of Dr. Thomas Mazzuchi of the Department of Engineering Management and Systems Engineering, George Washington University (GWU). Taking part in this research is entirely voluntary. Your academic standing or the status of your employment will not, in any way, be affected should you choose not to participate or if you decide to withdraw from the study at any time. Further information regarding this study may be obtained by contacting John Waxler (principal contact / co-investigator) at telephone number (610)-220-5726.

The purpose of this study is to use TOPSIS, a multi criteria decision making method, to prioritize security controls for home users.

If you choose to take part in this study, you will be asked to take a survey in which you will rate the security impact of exploit, time to exploit, and various cost factors for each security control presented. You will also be given space to make comments about each control. The total amount of time you will spend in connection with this study is about 45 minutes.. You may refuse to answer any of the questions and you may stop your participation in this study at any time.

Possible risks or discomforts you could experience during this study include: Loss of Confidentiality and Psychological Stress. However, every effort will be made to keep responses confidential.

You will not benefit directly from your participation in the study. The benefits to science and humankind that might result from this study are: 1. A systematic way to select security controls for implementation. 2. An increase in cyber security of systems implementing this method. 3. The creation of a prioritized list of security controls for home users.

Every effort will be made to keep your information confidential, however, this can not be guaranteed. Results will be collected by digital submission. Results will be saved on principal contact’s personal computer then encrypted/password protected. If results of this research study are reported in journals or at scientific meetings, the people who participated in this study will not be named or identified.

The Office of Human Research of George Washington University, at telephone number (202) 994-2715, can provide further information about your rights as a research participant.

Your willingness to participate in this research study is implied if you proceed.

*Please keep a copy of this document in case you want to read it again.

Are you willing to participate in this study?

*

○ Yes

○ No

2. Survey Overview

This survey asks 6 questions about each of 16 security controls. That is 96 questions in all. An answer must be selected for each question; however, the survey allows the users to select "Other (Please Specify)" for any question. Please select this answer if you would prefer not to answer a given question. If a participant is unsure of an answer he/she is encouraged to make an educated guess using professional judgement. Please use "Other" as a last resort. After the 6 questions, there is a place to leave additional comments about the control. The answers to these questions heavily depend on the user's habits and other external factors; however, you are asked to make your selections for what you consider an average user.

The goal of this research is to show how surveys can be used with systems engineering techniques to prioritize security controls. The 16 security controls selected are modified versions of the National Institute of Standards and Technology (NIST) security controls from Special Publication 800-53 Revision 4. Controls were selected and modified that are most applicable to home users.

When completing this survey please focus on how these controls would affect users in a home environment. The impact and priority of controls could be very different at home as opposed to in a corporate or government setting. Whenever possible the wording NIST used in the original control was preserved. In this survey, "organization" refers to the person making computer security decisions for a home computer.

In the first section, this survey asks about the participant's computer security experience and education.

NOTE: Asterisks (*) in this survey denote a required question. This is built in feature of the webpage providing the survey.

3. Information Security Experience and Qualifications

1. How many years of experience to do you have in the field of information security (This includes but is not limited to Information Security, Security Engineering, Cyber Security, System Administration, Information Technology with a security focus, Security Architect, Computer Forensics, and Malware Analyst.)?

2. What degrees, courses, certifications, and/or other training have you completed in information security?

4. Survey Control Questions Layout

The following web pages each consist of a tailored security control title followed by a list of applicable NIST security controls. After that, a detailed description of the tailored control is provided. Lastly, the participant is asked 6 questions about the tailored control and is provided a place to leave additional comments.

5. Account Management

Applicable NIST controls: AC-2, AC-6, IA-1

Description: The organization (Remember in this survey organization refers to the home user environment):

1. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
   a. Identifies and selects the right type of account (Administrator, User, etc.) for each user (ensures least privilege being enforced (AC-6))
   b. Ensures account requires a password or other form of authentication. (AC-3)
2. Creates, enables, modifies, disables, and removes information system accounts as required.

1. **What is the likely impact to security if this control is <u>not</u> implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?
*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.
○ Over 10 minutes but less than 1 hour.
○ Over 1 hour but less than 2 hours.
○ Over 2 hours but less than 4 hours.
○ Over 4 hours but less than 8 hours.
○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7. **Provide any comments or additional information regarding this control. Please elaborate on any questions you answered other above.**

6. Session Lock
Applicable NIST controls: AC-11

Description: The information system:
1. Prevents further access to the system by initiating a session lock after a defined time period of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.
○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.
○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.
○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.
○ Greater than 1 day but less than 1 week.
○ Greater than 1 week but less than 1 month.
○ Greater than 1 month but less than 1 year.
○ Over 1 year.
○ Other (Please Specify)

3.

What is the expertise required to implement this control with access

to basic online instructions?

*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.

○ Over 10 minutes but less than 1 hour per month.

○ Over 1 hour but less than 2 hours per month.

○ Over 2 hours but less than 4 hours per month.

○ Over 4 hours but less than 8 hours per month.

○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.

○ The risk is low impact or unlikely to occur.

○ The risk is high impact and/or likely to occur.

○ Other (Please Specify)

7. **Please provide any comments or additional information you have regarding this control.**

7. Wireless Access
Applicable NIST controls: AC-18

Description: The organization:
1. Ensures strong wireless encryption
2. Ensures strong passwords
3. Only allows authorized devices to connect to wireless network
a. Control password
4. Disables wireless capabilities on devices that don’t use wireless

1. **What is the likely impact to security if this control is <u>not</u> implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?
*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.

○ Over 10 minutes but less than 1 hour per month.

○ Over 1 hour but less than 2 hours per month.

○ Over 2 hours but less than 4 hours per month.

○ Over 4 hours but less than 8 hours per month.

○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.

○ The risk is low impact or unlikely to occur.

○ The risk is high impact and/or likely to occur.

○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.

8. Information Sharing
Applicable NIST controls: AC-21, AC-22

Description:
1. Create and disseminate an information sharing policy (This generally means discussing what shouldn’t be shared on the web including social media sites, blogs, etc.)

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?

*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7. **Please provide any comments or additional information you have regarding this control.**

9. Security Awareness Training

Applicable NIST controls: AT-2

Description: The organization provides or encourages basic security awareness training to information system users (parents, children, etc.):
1. Whoever is administering the computer (installing applications, setting up account, etc.) should understand the basic of administering the computer and security.
2. People using the computer should understand basic user functions. (They should be aware of things like fishing, exposing personal information, untrustworthy websites, etc.)

1. **What is the likely impact to security if this control is <u>not</u> implemented?** *

○ There is likely to be no loss in security.
○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination

of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?

*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7. **Please provide any comments or additional information you have regarding this control.**

10. Audit and Accountability
Applicable NIST controls: AU-1, AU-2, AU-4

Description: The organization:
1. Has a checklist of items to audit

2. The list should include but is not limited to:
a. Application of patches
b. Up to date definitions/signature files (specifically antivirus and malware protection)
c. Hard drive space (local, remote, backup, etc.)

1. **What is the likely impact to security if this control is <u>not</u> implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?
*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)?

Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.
○ Over 10 minutes but less than 1 hour.
○ Over 1 hour but less than 2 hours.
○ Over 2 hours but less than 4 hours.
○ Over 4 hours but less than 8 hours.
○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7. **Please provide any comments or additional information you have regarding this control.**

11. Configuration Management

Applicable NIST controls: CM-1, CM-2, CM-3, CM-5, CM-7, CM-10, CM-11

Description: The organization adheres to a configuration management policy. At minimum it should include:

1. What software is installed
2. Who is authorized to install software
3. What hardware is authorized to attach to a system
4. Who is authorized to add hardware to a system

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?
*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.
○ Over 10 minutes but less than 1 hour.
○ Over 1 hour but less than 2 hours.
○ Over 2 hours but less than 4 hours.
○ Over 4 hours but less than 8 hours.
○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.

○ The risk is high impact and/or likely to occur.

○ Other (Please Specify)

7. **Please provide any comments or additional information you have regarding this control.**

12. Configuration Settings
Applicable NIST controls: CM-6, CM-7

Description: The organization considers and documents how the operating system and applications are configured. Also, identifies who can change these settings and how often settings are verified.

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?
*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.
○ Over 10 minutes but less than 1 hour.
○ Over 1 hour but less than 2 hours.
○ Over 2 hours but less than 4 hours.
○ Over 4 hours but less than 8 hours.
○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)

*

○ There is no risk in implementing this control.

○ The risk is low impact or unlikely to occur.

○ The risk is high impact and/or likely to occur.

○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.

13. Contingency Planning

Applicable NIST controls: CP-1, CP-2, CP-6, CP-10, IR-1, IR-1, IR-4

Description: The organization describes what steps to be taken in case of a computer failure (including but not limited to complete system failure, data loss, component failure, etc.). This should be part a contingency plan that may or may not be written. Particular thought should be given to:

1. If System/Data Backups are taken. If they are taken, thought should be given to the restoration process.
2. If outside resources are needed they should be identified.

1. **What is the likely impact to security if this control is <u>not</u> implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?

*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.

○ Over 10 minutes but less than 1 hour per month.

○ Over 1 hour but less than 2 hours per month.

○ Over 2 hours but less than 4 hours per month.

○ Over 4 hours but less than 8 hours per month.

○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.

○ The risk is low impact or unlikely to occur.

○ The risk is high impact and/or likely to occur.

○ Other (Please Specify)

7. **Please provide any comments or additional information you have regarding this control.**

14. System Maintenance Policy and Procedures
Applicable NIST controls: MA-1, MA-6

Description: The organization:
1. Plans when upgrades (hardware and software) should be performed
2. Has a regular updating and patching policy

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?

*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.

○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.

15. Media Protection
Applicable NIST controls: MP-1, MP-2, MP-6, SC-28

Description: Media (including but not limited to hard drives, CDs, DVDs, etc.) is protected appropriately.
1. Sensitive information is encrypted
2. Media is stored and transported in accordance with organizational policy based on the data it holds
3. Media is sanitized before disposal or when otherwise appropriate.

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.
○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination

of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?

*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)

*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.

16. Risk Assessment

Applicable NIST controls: RA-1, RA-5

Description: The organization has a risk assessment policy. This takes into consideration criticality of the system and its data when implementing security controls. Vulnerability scanning may help assess the risk of the system.

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?
*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to

initial implementation and not maintenance time.

*

○ Less than 10 minutes.
○ Over 10 minutes but less than 1 hour.
○ Over 1 hour but less than 2 hours.
○ Over 2 hours but less than 4 hours.
○ Over 4 hours but less than 8 hours.
○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)

*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.

17. System and Service Acquisition
Applicable NIST controls: SA-1

Description: Organization considers the reputation of the companies from which they purchase systems and services. The organization considers that items they purchase could contain malware and the people providing services may have malicious intent.

1. **What is the likely impact to security if this control is <u>not</u> implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?
*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.
○ Over 10 minutes but less than 1 hour.
○ Over 1 hour but less than 2 hours.
○ Over 2 hours but less than 4 hours.
○ Over 4 hours but less than 8 hours.
○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)

*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.

18. Boundary Protection
Applicable NIST controls: SC-7

Description: The information system:
a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices (Example: Firewall) arranged in accordance with an organizational security architecture.

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.

○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.

○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?

*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.

○ Over 10 minutes but less than 1 hour per month.

○ Over 1 hour but less than 2 hours per month.

○ Over 2 hours but less than 4 hours per month.

○ Over 4 hours but less than 8 hours per month.

○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.

19. Transmission Confidentiality and Integrity
Applicable NIST controls: SC-8

Description: The information system protects the confidentiality and/or integrity of transmitted information. (Examples: Utilizes encryption like HTTPS, VPN, PGP, etc.)

1. **What is the likely impact to security if this control is <u>not</u> implemented?** *

○ There is likely to be no loss in security.
○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.
○ There is likely to be a total loss of confidentiality, integrity, or accessibility or a partial loss that has a direct and serious consequence.
○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.
○ Greater than 1 day but less than 1 week.
○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?

*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.

○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)
*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.

20. Malicious Code Protection

Applicable NIST controls: SI-3, SI-8

Description: The organization:
a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. This includes decreasing the likelihood of exposure to malicious code. For example spam protection and careful browsing.

1. **What is the likely impact to security if this control is not implemented?** *

○ There is likely to be no loss in security.
○ There is likely to be a partial loss of security. Some part of the system may have a loss of confidentiality, integrity, accessibility, or any combination of three.
○ There is likely to be a total loss of confidentiality, integrity, or accessibility

or a partial loss that has a direct and serious consequence.

○ Other (Please Specify)

2. **How long does it take before this condition is likely to be exploited?** *

○ Less than 1 day.

○ Greater than 1 day but less than 1 week.

○ Greater than 1 week but less than 1 month.

○ Greater than 1 month but less than 1 year.

○ Over 1 year.

○ Other (Please Specify)

3.

What is the expertise required to implement this control with access to basic online instructions?
*

○ PC User: For example, the user knows how to login into their account, browse the web, and edit documents.

○ Administrative User: For example, the administrator knows how to add/remove programs, manage system accounts, update applications, and avoid suspect websites.

○ Security Expert: For example, the security expert knows how to modify access controls, create group policy, and administer malware protection,.

○ Other (Please Specify)

4.

How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.

*

○ Less than 10 minutes.

○ Over 10 minutes but less than 1 hour.

○ Over 1 hour but less than 2 hours.

○ Over 2 hours but less than 4 hours.

○ Over 4 hours but less than 8 hours.

○ Other (Please Specify)

5.

How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?

*

○ Less than 10 minutes per month.
○ Over 10 minutes but less than 1 hour per month.
○ Over 1 hour but less than 2 hours per month.
○ Over 2 hours but less than 4 hours per month.
○ Over 4 hours but less than 8 hours per month.
○ Other (Please Specify)

6.

What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of accessibility.)

*

○ There is no risk in implementing this control.
○ The risk is low impact or unlikely to occur.
○ The risk is high impact and/or likely to occur.
○ Other (Please Specify)

7.

Please provide any comments or additional information you have regarding this control.