

Automated IT Audit of Windows Server Access Control

Sutthinee PONGSRISOMCHAI, Sudsanguan NGAMSURIYAROJ

Faculty of Information and Communication Technology, Mahidol University, Thailand

spongsrisomchai@gmail.com, sudsanguan.nga@mahidol.ac.th

Abstract— To protect sensitive information of an organization, we need to have proper access controls since several data breach incidents were happened because of broken access controls. Normally, the IT auditing process would be used to identify security weaknesses and should be able to detect any potential access control violations in advance. However, most auditing processes are done manually and not performed consistently since lots of resources are required; thus, the auditing is performed for quality assurance purposes only. This paper proposes an automated process to audit the access controls on the Windows server operating system. We define the audit checklist and use the controls defined in ISO/IEC 27002:2013 as a guideline for identifying audit objectives. In addition, an automated audit tool is developed for checking security controls against defined security policies. The results of auditing are the list of automatically generated passed and failed policies. If the auditing is done consistently and automatically, the intrusion incidents could be detected earlier and essential damages could be prevented. Eventually, it would help increase the reliability of the system.

Keywords—IT Audit, Access Control, Windows Server, Automated Audit Tool

I. INTRODUCTION

Today, technologies, businesses, laws and regulations in the world have changed rapidly in a very drastic way. Several companies have to deal with emerging challenges daily. In addition, over the last few years, cybersecurity threats become the top technology challenges as many organizations are under attacks. Insider threats are the key concern for data breaches in organizations, especially when servers are the target of attacks by disgruntled employees or outsource vendors [1].

Thus, conducting security audit of operating systems has become a mandatory task in IT audit processes. A recent global survey [2] shows that significant challenges in IT auditing of an organization are “In-house internal audit department lacks IT audit skill sets” and “lack of resources”.

In addition, the audit process needs to be improved because most audit activities are manually operated. Moreover, lack of standards or practices applied in an audit checklist could lead to unreliable audit results.

In this paper, we propose an automated process developed for auditing access controls of the Windows server operating system since the Windows operating system is one of the most widely used operating systems in industries. In addition, doing manual auditing could not provide consistency in auditing quality and would need lots of resources. Our work provides

the automated auditing process which applied the leading information security standard ISO/IEC 27002:2013 as a guidance for identifying audit objectives.

The results would give the following benefits to auditors and organizations.

- Increasing the auditing productivity by reducing time and efforts
- Providing consistency in the auditing quality by reducing manual processes
- Providing reliability and traceability of audit work since all audit evidences and results are kept in a database. Moreover, relevant information such as security policies, current configurations on servers and audit results are included in our audit reports.

Thus, our work could help enhance the productivities and the qualities of the security audit of the Windows server access controls. The contributions include applying security management techniques and performing log analysis. It also can be implemented with limited budget.

The remainder of the paper is organized as follows. Section 2 gives the related work. Section 3 presents the proposed work. Section 4 describes the implementation and the results. Finally, concluding remarks are given in Section 5.

II. RELATED WORK

The access control is the primary concern of security breaches which caused by insiders [1]. Those insiders could be privileged users such as administrators, third-party vendors or terminated employees. The consequences of such threats could be data leakage or data misuse.

From several related works, servers are potential targets for attacks [3] since sensitive business data are usually stored in computer systems [4]. In addition, customers and other confidential information are the major concerns for organization. Operating system auditing should be performed carefully for maintaining confidentiality, integrity and availability of systems and data for business [4].

Effectiveness of access controls over an operating system can help organizations to reduce the potentials of cyber-attacks. The authors in [3] have implemented an automated tool for supporting system administrators with the limited purposes of auditing servers against the predefined security policies.

III. PROPOSED WORK

The overview of the proposed model as shown in the Figure 1 consists of three steps: the audit checklist for Windows access controls, the automated auditing, and the audit report generation.

First, to define the audit checklist, we use the controls defined in ISO/IEC 27002:2013 [7] as a guidance to identify audit objectives. Next, an automated audit tool is developed for checking security controls based on the audit objectives specified in the audit checklist. The tool can be used for enhancing the productivity, the consistency in audit quality, as well as the reliability and traceability of the audit works. Finally, the audit results are automatically generated. The details of each step are explained as follows.

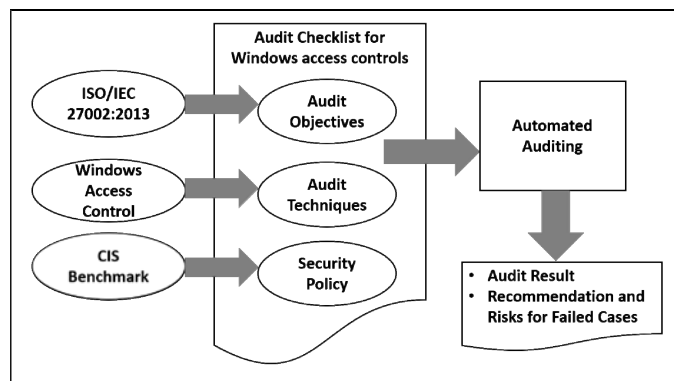


Figure 1. The Overview of Proposed Model

A. Audit Checklist for Windows Access Controls

In the IT audit process [5], auditors normally develop the audit checklist or so-called the audit work program during the audit planning phase. The adequate audit planning could help ensure that the important areas of the audit will be considered by auditors. There are three steps for developing the audit checklist.

1) Identifying audit objectives: We identify the audit objectives based on 14 access controls given in Section A.9 ISO/IEC 27001:2013 Annex A [6].

2) Identifying audit techniques: From our study of Windows access controls, we identify audit techniques to obtain audit evidences including the configuration of Group Policy, User ID, User Right Assignment, Audit Policy, Password Policy, Account Policy, Personalization setting, Security Option setting, Permission of files and folders and Windows event logs to support the defined audit objectives.

3) Identifying security policy: We adopt the CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark [8] as a guideline to develop our security policy. The CIS Benchmark provides the detailed guidance for implementing secure configuration on Windows Server as they are the recommended security configuration for Windows Server. In this paper, we define 53 security policies to serve our audit objectives. Among them, 47 security policies can be fully automated auditing and 6 security policies can be partially

automated auditing where auditors must review before concluding the audit results. The details of our audit objectives and security policies are described as follows.

A.9.1.1 Access Control Policy

Audit Objective: Check whether Group policy is established and applied on Windows Active Directory.

Security Policy: [SP-01] Group policy should be established and applied from Windows Active Directory to maintain the security level for the entire Windows domain.

A.9.1.2 Access to networks and network services

Audit Objective: Check whether the parameters of User Rights Assignment relating to network accesses are appropriately configured according to the access control policy or a standard guideline.

Security Policy: The following policies are defined to determine the security of network accesses.

- [SP-02] Accessing a computer from the network should be restricted to Administrators, Authenticated Users and Enterprise Domain Controllers.
- [SP-03] Denying an access to a computer from the network should be assigned to Guests.
- [SP-04] Allowing log on through Remote Desktop Services should be restricted to Administrators and Remote Desktop Users.
- [SP-05] Denying log on through Remote Desktop Services should be assigned to Guests.

A.9.2.1 User registration and de-registration

Audit Objective: Check whether all User IDs on the operating system are unique and check whether there are no redundant User IDs.

Security Policy:

- [SP-20] User IDs should be unique.
- [SP-21] One user should own only one User ID in a system.

A.9.2.2 User access provisioning

Audit Objective: Filter and list all event logs of access assignment and access revocation to check whether they are authorized.

Security Policy:

- [SP-26] Access assignment should be approved based on the company's policy before configuring on the operating system.
- [SP-27] Access revocation should be approved based on the company's policy before configuring on the operating system.

The audit processes of [SP-26] and [SP-27] are partially automated. Auditors need to review the event logs against the approval of access assignment and revocation.

A.9.2.3 Management of privileged access rights

Audit Objective: List all privileged User IDs on the operating system to check whether they are authorized.

Security Policy: [SP-24] Privileged User IDs should be restricted to only authorised persons with corresponding job responsibilities. The audit processes of this policy are partially automated. Auditors need to review the privileged User IDs against the approval of privileged access assignment.

A.9.2.4 Management of secret authentication information of users

Audit Objective: Check whether forcing user change password at the first logon is set for all User IDs.

Security Policy: [SP-22] All User IDs on the operating system should be set Force User Change Password at the first logon to maintain the secret of password.

A.9.2.5 Review of user access rights

Audit Objective: Check whether audit logs of access assignment and access revocation are enabled and retained.

Security Policy: The following policies are defined to determine whether the relevant audit logs of access assignment and revocation are kept for reviews.

- [SP-28] Audit User Account Management, this parameter should be set as Success and Failure.
- [SP-29] Audit Security Group Management, this parameter should be set as Success and Failure.

A.9.2.6 Removal or adjustment of access rights

Audit Objective: Check whether no resign employee's User ID is active on the operating system.

Security Policy: [SP-19] Resign employees should not be active on the operating system to prevent unauthorized uses. The User ID of resign employees need to be configured in this policy.

A.9.3.1 Use of secret authentication information

Audit Objective: Three objectives are identified as follows,

- Check whether all User IDs on O/S are set the password expiration.
- Check whether the Windows logon screen is set to prevent displaying last account name of last user who logged on the server.
- Check whether the Windows logon screen is set to prevent displaying password in plain text while user types a password.

Security Policy:

- [SP-23] All User IDs should be set password expiration to enhance the security of password.
- [SP-35] Interactive logon: Do not display last user name, this parameter under security option should be enabled.
- [SP-39] Credential User Interface: Do not display the password reveal button, this parameter under Windows component should be enabled.

A.9.4.1 Information access restriction

Audit Objective: Check whether the parameters of User Rights Assignment relating to system and application accesses are appropriately configured according to a company access control policy or a standard guideline.

Security Policy: The following policies are defined to determine the security of system and application accesses.

- [SP-06] Allow log on locally, this right should be restricted to Administrators and ENTERPRISE DOMAIN CONTROLLERS.
- [SP-07] Deny log on as a batch job, this right should be assigned to Guests.
- [SP-08] Deny log on as a service, this right should be assigned to Guests.

- [SP-09] Deny log on locally, this right should be assigned to Guests.
- [SP-10] Log on as a batch job, this right should be restricted to Administrators.
- [SP-11] Log on as a service, this right should not be assigned to anyone.
- [SP-12] Access credential manager as a trusted caller, this right should not be assigned to anyone.
- [SP-13] Act as part of the operating system, this right should not be assigned to anyone.
- [SP-14] Create a token object, this right should not be assigned to anyone.
- [SP-15] Enable computer and user accounts to be trusted for delegation, this right should be restricted to Administrators.
- [SP-16] Generate security audits, this right should be restricted to LOCAL SERVICE and NETWORK SERVICE
- [SP-17] Impersonate a client after authentication, this right should be restricted to Administrators, LOCAL SERVICE, NETWORK SERVICE and SERVICE.
- [SP-18] Manage auditing and security log, this right should be restricted to Administrators.

A.9.4.2 Secure log-on procedures

Audit Objective: Five objectives are identified as follows,

- Check whether the name of administrator and guest accounts are changed because they are default Windows accounts.
- Check whether the account lockout policy is appropriately set according to a company access control policy or a standard guideline.
- Check whether audit logs of unsuccessful and successful logon on O/S are enabled and retained.
- Check whether the setting of automatically log off users after a defined period of inactivity is appropriately configured according to a company access control policy or a standard guideline.
- Check whether the setting of screen locks on the system is appropriately configured according to a company access control policy or a standard guideline to prevent unauthorized access.

Security Policy: The following policies are defined to determine the security of log-on procedures.

- [SP-30] Logon/Logoff: Logon, this parameter should be set as Success and Failure.
- [SP-31] Logon/Logoff: Logoff, this parameter should be set as Success.
- [SP-32] Logon/Logoff: Account Lockout, this parameter should be set as Success.
- [SP-33] Logon/Logoff: Special Logon, this parameter should be set as Success.
- [SP-34] Privilege Use: Sensitive Privilege Use, this parameter should be set as Success and Failure.
- [SP-36] Accounts: Rename administrator account, the value of this parameter should not be Administrators.
- [SP-37] Accounts: Rename guest account, the value of this parameter should not be Guest.

- [SP-38] Interactive logon: Machine inactivity limit, this parameter should be set as 900 (minutes) or fewer, but not equal 0 (disabled).
- [SP-40] Enable screen saver, this parameter should be enabled.
- [SP-41] Password protect the screen saver should be enabled.
- [SP-42] Screen saver timeout, this parameter should be set as 900 (minutes) or fewer, but not equal 0 (disabled).
- [SP-49] Account Lockout Policy: Account lockout duration, this parameter should be set as 15 (minutes) or longer.
- [SP-50] Account Lockout Policy: Account lockout threshold, this parameter should be set as 10 (invalid logon attempts) or fewer but not equal 0 (disabled).
- [SP-51] Account Lockout Policy: Reset account lockout counter after, this parameter should be set as 15 (minutes) or longer.

A.9.4.3 Password management system

Audit Objective: Check whether password policy and account policy on O/S are appropriately set according to a company access control policy or a standard guideline.

Security Policy: The following policies are defined to determine the security of password.

- [SP-43] Password Policy: Enforce password history, this parameter should be set as 24 or more than.
- [SP-44] Password Policy: Maximum password age, this parameter should be set as 60 (days) or fewer but not equal 0 (disabled).
- [SP-45] Password Policy: Minimum password age, this parameter should be set as 1 or more than.
- [SP-46] Password Policy: Minimum password length, this parameter should be set as 14 or more than.
- [SP-47] Password Policy: Password must meet complexity requirements, this parameter should be enabled.
- [SP-48] Password Policy: Store passwords using reversible encryption, this parameter should be disabled.

A.9.4.4 Use of privileged utility programs

Audit Objective: Filter and list Users IDs which have local administrator's right to check whether they are authorized because this right give authorization of program installation on the operating system. Another objective is to filter and list all event logs of program installation to check whether there is any unauthorized installation on servers.

Security Policy:

- [SP-25] Local administrator's right should be restricted to authorized persons based on their job responsibilities. Inappropriate right assignment, malicious software programs could be installed on the operating system.
- [SP-52] All program installed on servers should be approved by authorized persons regarding the company's policy.

The audit processes of [SP-25] and [SP-52] are partially automated. Auditors need to review the User IDs which have local administrator's right against the approval of access assignment (e.g. form or any documents) and they need to

review the even logs against the approval list of authorized programs that allowed to install on servers.

A.9.4.5 Access control to program source code

Audit Objective: Filter and list all User IDs who can access to program source code (file/ directory) to check whether they are authorized persons.

Security Policy: [SP-53] Access to program source code should be restricted to authorized persons based on their job responsibilities to prevent unauthorized changes to program source code. The audit processes of this policy are partially automated. Auditors need to review the User IDs against the list of authorized persons.

B. Automated Audit Tool

The process of the automated auditing is depicted in Figure 2. The process will read the Windows logs and the settings of security configurations, examine them with the corresponding security policies, and put the results into the database before generating the audit reports. The details of the processes are described as follows.

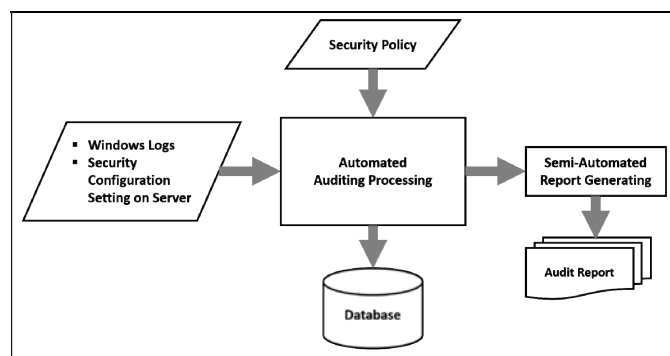


Figure 2. Automated Auditing Process

1) Audit Script: The audit script is developed using the PowerShell script to gather audit evidences on a server. The audit script retrieves the current values of the security configurations at the operating system level and Windows event logs according to the audit objectives. The outputs from running the audit script is text files.

2) Security Policy: The security policy is created as a text file containing the recommended values of each policy. The purpose is to use the recommended values as a baseline to check against the current settings of the security configuration's values on the Windows server as we have obtained from Step 1.

3) Audit Program: The program for compliance checking is developed using C# to analyze the outputs from Step 1 based on the security policy created in Step 2. The data analytic techniques including searching, filtering, comparing and checking for duplicated data are applied. The outputs of this step are the auditing results as Passed or Failed, and they are kept in the SQLite database. An alert report would be generated as a Microsoft Excel file providing the differences between the previous audit results and the current audit results.

The tool also has a function to export the audit results from the database as the Microsoft Excel files to be used in Step 4.

Figure 3 illustrates the sample summary audit report. The objective of this report is to briefly illustrate the audit results (Passed/ Failed) for each predefined security policy mapped with the ISO controls. In this example, there are 38 passed cases and 9 failed cases which we set the configuration's value differently from the recommended configuration's value defined in the security policies. For the failed cases, 7 security policies correspond to the ISO controls in A.9.4 System and Application Access Control, 1 security policy corresponds to the ISO controls in A.9.3 User Responsibilities and 1 security policy corresponds to the ISO controls in A.9.2 User Access Management.



Figure 3. Sample Summary Audit Report

4) Report Generator: The report generator is developed for creating the audit report as the document for the auditor. It is created by importing the audit results from the Excel files in Step 3 into the report generator's database and the report templates developed are selected to display the audit results. The three types of audit report templates are the Summary Audit Report listed by ISO Control, the Detailed Audit Report listed by security policies, and the Failed Cases Audit Report.

5) Database: The database contains four tables as follows,

- **ISO Master Table:** This table stores the details of the 14 access controls in ISO/IEC 27002:2013.
- **Audit Policy Master Table:** This table stores the master data of audit information and security policies as they are obtained from the audit checklist developed earlier.
- **Fully Automated Auditing Result Table:** This table stores the audit results of the security policies that can be fully automated auditing. The audit results include the current configuration's value configured in the operating system and the recommended configuration's value defined in the security policy.

- **Partially Automated Auditing Evidence Table:** This table stores the audit evidences for the security policies that can be partially automated auditing. In this case, auditors must review the audit evidences before concluding the audit results. The evidences are retrieved automatically by running the audit tool, and the data is the current configuration values.

After running the developed program, the results are displayed on the console as exemplified in Figure 4.

```
[INFO] ReadMachineName() : MachineName : AD001
[INFO] ReadMachineName() : Current UTC Time : 9/30/2018 1:59:03 PM
[INFO] QueryResult() : Query result from DB :
[INFO] QueryResult() : [SP01] Group Policy was applied from : PASSED
[INFO] QueryResult() : [SP02] SeNetworkLogonRight : PASSED
[INFO] QueryResult() : [SP03] SeDenyNetworkLogonRight : PASSED
[INFO] QueryResult() : [SP04] SeRemoteInteractiveLogonRight : PASSED
[INFO] QueryResult() : [SP05] SeDenyRemoteInteractiveLogonRight : PASSED
[INFO] QueryResult() : [SP06] SeInteractiveLogonRight : PASSED
[INFO] QueryResult() : [SP07] SeDenyBatchLogonRight : PASSED
[INFO] QueryResult() : [SP08] SeDenyServiceLogonRight : PASSED
[INFO] QueryResult() : [SP09] SeDenyInteractiveLogonRight : PASSED
[INFO] QueryResult() : [SP10] SeBatchLogonRight : FAILED
[INFO] QueryResult() : [SP11] SeServiceLogonRight : PASSED
[INFO] QueryResult() : [SP12] SeTrustedCredManAccessPrivilege : FAILED
[INFO] QueryResult() : [SP13] SeTcbPrivilege : FAILED
[INFO] QueryResult() : [SP14] SeCreateTokenPrivilege : FAILED
[INFO] QueryResult() : [SP15] SeEnableDelegationPrivilege : PASSED
[INFO] QueryResult() : [SP16] SeAuditPrivilege : FAILED
[INFO] QueryResult() : [SP17] SeImpersonatePrivilege : FAILED
[INFO] QueryResult() : [SP18] SeSecurityPrivilege : PASSED
[INFO] QueryResult() : [SP19] User name : PASSED
```

Figure 4. Sample Results of Running Audit Program

IV. IMPLEMENTATION AND RESULTS

In the implementation, we used C# and PowerShell scripts for developing the automated audit tool to check whether the configurations setting on Windows servers comply with our predefined security policies. The auditing results from the tool are presented as the audit reports. In our experiment, we have one Active Directory and 3 servers running Windows Server 2016 Datacenter 64-bit version. Moreover, we generate the test data by simulating a set of events of passed and failed cases on the test servers to evaluate the correctness of the audit results provided by our automated audit tool.

The tool is also scheduled to run periodically on those servers. The results show that the tool can automatically detect and report the configurations which do not comply with the predefined security policies and it automatically generates alerts of changes by comparing the current audit results with the previous ones. In addition, we conducted six audit rounds. The tool generates the audit results and alerts as shown in Table 1 and Table 2.

For example, in the 1st round, the audit results show that the number of failed cases is 15 and the number of alerts is 0. In the 2nd round, the audit results show that there is no failed case and the tool generates 15 alerts. It means that 15 security policies had changed from the 1st round. Thus, the corresponding results are changed from "Failed" to "Passed". In addition, the results from the experiment show that the tool can check security configurations related to Windows access control defined based on the security controls in ISO/IEC 27002:2013. The results also show the capability of active auditing for the Windows security access control, detecting the security weaknesses and notifying the alerts in a timely manner.

TABLE 1. SAMPLE OF AUDIT RESULTS

Round No.	Audit Results of 47 Security Policies		
	% of Pass Cases	Number of Failed Cases	Security Policy of Failed Cases
1	68.09%	15	SP-01, SP-19, SP-20, SP-21, SP-22, SP-23, SP-28, SP-29, SP-30, SP-31, SP-32, SP-33, SP-34, SP-35, SP-36
2	100%	0	None
3	48.94%	24	SP-12, SP-13, SP-19, SP-22, SP-23, SP-30, SP-31, SP-32, SP-33, SP-37, SP-38, SP-39, SP-40, SP-41, SP-42, SP-43, SP-44, SP-45, SP-46, SP-47, SP-48, SP-49, SP-50, SP-51
4	76.60%	11	SP-06, SP-11, SP-12, SP-13, SP-19, SP-20, SP-37, SP-38, SP-39, SP-49, SP-50
5	61.70%	18	SP-02, SP-03, SP-04, SP-05, SP-06, SP-07, SP-08, SP-09, SP-10, SP-11, SP-12, SP-13, SP-14, SP-15, SP-16, SP-17, SP-18, SP-19
6	85.11%	7	SP-19, SP-43, SP-44, SP-45, SP-46, SP-47, SP-48

V. CONCLUSIONS

In this paper, the audit checklist and the automated audit tool are developed to enhance the productivities and the qualities of security audit of Windows server access controls. The manual tasks for auditing could be eliminated and the resources and time spent could be reduced as well. In addition, any organization lacking skilled IT auditors could use our audit checklist and tool with minimum cost. Our approach could also be adopted to develop in-house tools for performing other IT audit works including the security audit of Linux operating system, or the security audit on database systems or applications.

ACKNOWLEDGMENT

This research work was partially supported by the Faculty of Information and Communication Technology, Mahidol University.

REFERENCES

- [1] Verizon, *2017 Data Breach Investigations Report*, 10th ed., 2017.
- [2] ISACA and Protiviti, *A Global look at IT Audit Best Practices; Assessing the International Leaders in an Annual ISACA/Protiviti Survey*, 6th Annual IT Audit Benchmarking Survey, 2017.
- [3] Sonali Patra, N C Naveen and Omkar Prabhakar, "An Automated Approach For Mitigating Server Security Issues," *IEEE International Conference on Recent Trends in Electronics Information Communication Technology*, p. 1075–1079, 2016.
- [4] Aateqaa Al Lawati and Saqib Ali, "Business Perception to Learn The Art of Operating System Security Auditing: A Case of A Local Bank of Oman," *IEEE 8th GCC Conference and Exhibition*, p. 1–6, 2015.
- [5] ISACA, *ITAF A Professional Practices Framework for IS Audit/Assurance*, 3rd ed., 2014.
- [6] ISO and IEC, *International Standard ISO/IEC 27001:2013*, 2nd ed., 2013.

TABLE 2. SAMPLE OF ALERTS

Round No.	Total Alerts	Type of Alerts	
		Passed to Failed	Failed to Passed
1	0	None	None
2	15	None	(15 Security Policies) SP-01, SP-19, SP-20, SP-21, SP-22, SP-23, SP-28, SP-29, SP-30, SP-31, SP-32, SP-33, SP-34, SP-35, SP-36
3	24	(24 Security Policies) SP-12, SP-13, SP-19, SP-22, SP-23, SP-30, SP-31, SP-32, SP-33, SP-37, SP-38, SP-39, SP-40, SP-41, SP-42, SP-43, SP-44, SP-45, SP-46, SP-47, SP-48, SP-49, SP-50, SP-51	None
4	19	(3 Security Policies) SP-06, SP-11, SP-20	(16 Security Policies) SP-22, SP-23, SP-30, SP-31, SP-32, SP-33, SP-40, SP-41, SP-42, SP-43, SP-44, SP-45, SP-46, SP-47, SP-48, SP-51
5	19	(13 Security Policies) SP-02, SP-03, SP-04, SP-05, SP-07, SP-08, SP-09, SP-10, SP-14, SP-15, SP-16, SP-17, SP-18	(6 Security Policies) SP-20, SP-37, SP-38, SP-39, SP-49, SP-50
6	23	(6 Security Policies) SP-43, SP-44, SP-45, SP-46, SP-47, SP-48	(17 Security Policies) SP-02, SP-03, SP-04, SP-05, SP-06, SP-07, SP-08, SP-09, SP-10, SP-11, SP-12, SP-13, SP-14, SP-15, SP-16, SP-17, SP-18

[7] ISO and IEC, *International Standard ISO/IEC 27002:2013*, 2nd ed., 2013.

[8] Center of Internet Security (CIS), *CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark*, v1.0.0, 2017.



Sutthinee Pongsrisomchai received her B.Sc. degree in Computer Science from Kasetsart University, Thailand in 2007 and currently a Master student in Cybersecurity and Information Assurance program at the Faculty of ICT at Mahidol University, Thailand.



Sudsanguan Ngamsuriyaroj is now an associate professor at Mahidol University. She received her Ph.D. degree in Computer Science and Engineering from Pennsylvania State University, USA. Her research interests include network security, cloud security, and IoT security. Her research projects include IoT energy and healthcare applications especially for rehabilitation medicine.