ความเสี่ยงและผลกระทบต่อผู้สอบบัญชีเมื่อบริษัทใช้งาน Cloud

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

หัวข้อ

- บทนำ
  - อะไรคือ Cloud
  - On-Premises vs. Cloud
  - ประเภทของ Cloud
- ทำไมผู้สอบบัญชีควรเข้าใจถึงความเสี่ยงของการใช้งาน Cloud
- รายงาน SOC
  - ประเภทของ SOC Report
  - ตัวอย่างรายงาน SOC Report
- ตรวจสอบการควบคุมของบริษัทที่ใช้ Cloud

บทนำ

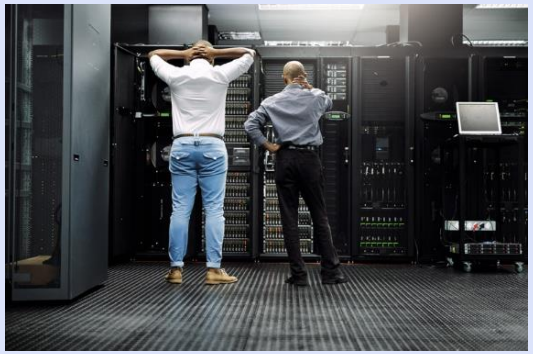
บทนำ อะไรคือ Cloud

- Cloud คือการให้บริการด้าน Computing Service เช่น Servers, databases, network, software ผ่านทาง Internet (ตัวอย่าง Office365, Google Drive, One drive, aws, dropbox, iCloud)

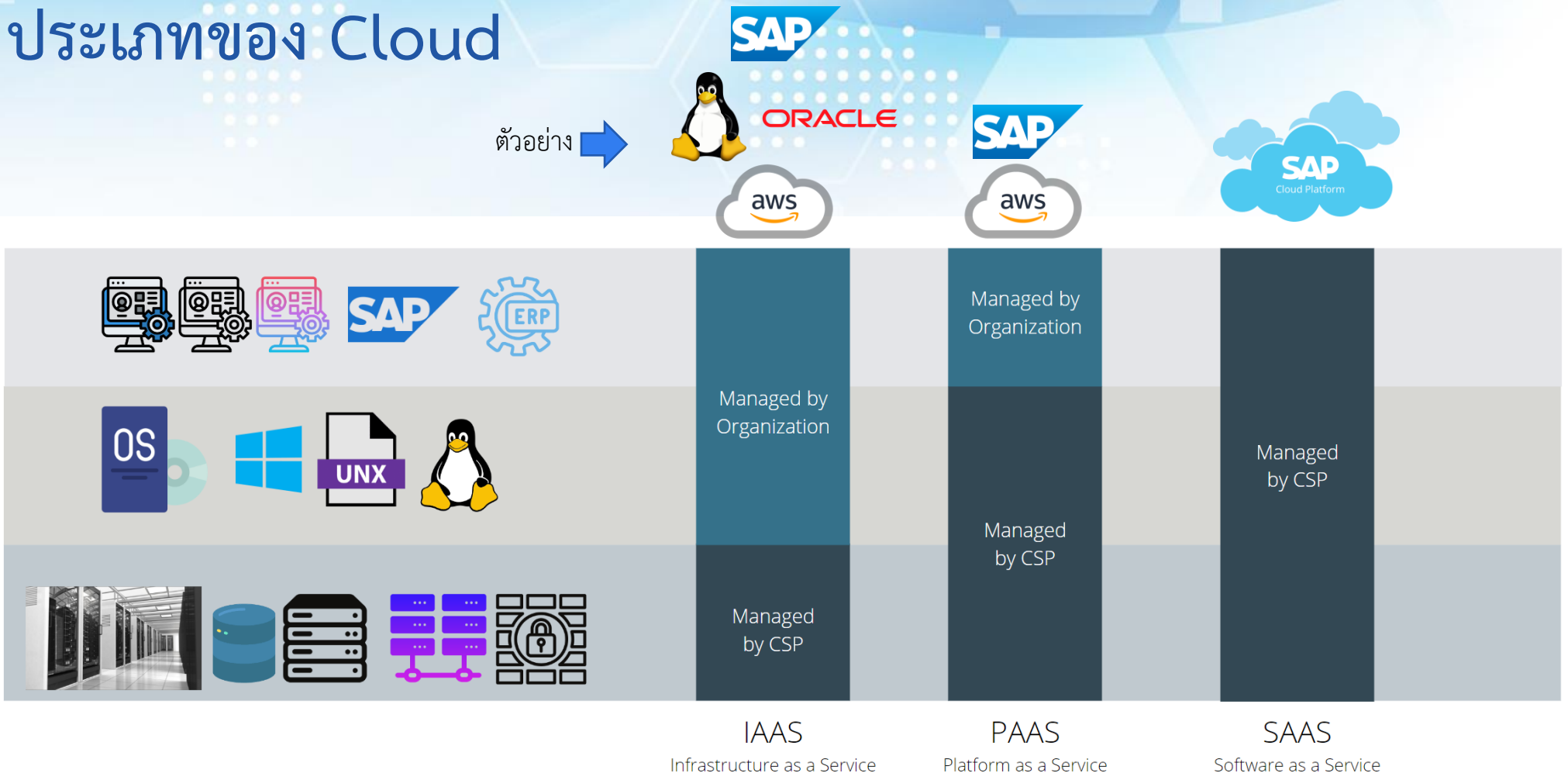
- Cloud Service Provider (CSP) เป็นผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ ประเภทนึง

- การใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT Outsourcing) หมายความว่า การใช้บริการจากผู้ให้บริการภายนอกในการดำเนินการด้านงานเทคโนโลยีสารสนเทศให้แก่บริษัท ซึ่งโดยปกติแล้วบริษัทต้องดำเนินการเอง

On-Premises vs. Cloud

On-Premises	Cloud
• ระบบงานและ Data Center ดูแลและจัดการโดยเจ้าหน้าที่ของบริษัทและจัดตั้งอยู่ในสถานที่ของบริษัทเอง • ยากต่อการขยับขยาย เปลี่ยนแปลง โอนย้าย • มีค่าใช้จ่ายด้าน Infrastructure (อาคาร ห้อง Data Center, Fire prevention system) • มีค่าใช้จ่ายด้าน Data security • ความสามารถในการกู้ข้อมูล (Data recovery) ขึ้นอยู่กับการออกแบบการควบคุม • มีค่าใช้จ่าย Maintenance Agreement สำหรับ Server และ โครงสร้างของห้อง	• ระบบงาน หรือ Data Center โดยทั้งหมด หรือ บางส่วนดูแลและจัดการโดยผู้ให้บริการภายนอกและจัดตั้งอยู่ในสถานที่ของผู้ให้บริการภายนอก • จ่ายตามที่ใช้จริง (Pay on demand) • ง่ายต่อการปรับเปลี่ยนขนาด • มีความสามารถในการกู้ระบบงานที่รวดเร็ว • ค่าใช้จ่ายด้าน Data security ต่ำ • การบำรุงรักษา Server และ Infrastructure จัดทำโดยผู้ให้บริการ
	

ประเภทของ Cloud



ทำไมผู้สอบบัญชีควรเข้าใจถึงความเสี่ยงของการใช้งาน Cloud

ทำไมผู้สอบบัญชีควรเข้าใจถึงความเสี่ยงของการใช้งาน Cloud

- ทบทวนการควบคุมทั่วไปเทคโนโลยีสารสนเทศ

- การบริหารจัดการผู้ใช้งาน
- การตั้งค่าความปลอดภัยและรหัสผ่านระบบงาน
- การบริหารจัดการผู้ใช้งานที่สิทธิสูง
- การสอบทาน Log ด้านความปลอดภัยสารสนเทศ
- การบริหารจัดการการเปลี่ยนแปลงระบบ (Manage Change)
- การบริหารการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (Manage IT Operation)

ทำไมผู้สอบบัญชีควรเข้าใจถึงความเสี่ยงของการใช้งาน Cloud – ต่อ

- การใช้งาน Cloud Computing อาจมีความเสี่ยงด้าน IT General Control ที่เปลี่ยนไปและมีผลกระทบต่องบการเงิน

ผู้สอบบัญชีควร:

- ทำความเข้าใจว่าบริษัทใช้ Cloud Computing ประเภทอะไร และอย่างไร
- สอบทานการควบคุมของผู้ให้บริการ Cloud (CSP) ดังต่อไป
    1. สอบทาน SOC Report (ถ้ามี) ดูความเหมาะสมพอเพียงของรายงาน (หากไม่เพียงพอให้ทำข้อ 2)
    2. สอบทานการควบคุมที่ผู้ให้บริการ Cloud (CSP) โดยผู้ตรวจสอบเอง โดยประสานงานผ่านบริษัทฯ
- สอบทานการควบคุมการบริหารจัดการผู้ให้บริการภายนอกของบริษัท (IT Outsourcing Management)

การแบ่งแยกการควบคุมที่บริหารจัดการระหว่างบริษัท และ CSP เพื่อวางแผนตรวจสอบ

		IaaS on-premise	IaaS CSP	PaaS CSP	SaaS CSP
Software	Application Control	Audit Directly	Audit Directly	Audit Directly	Audit Directly
Platform	Application level (ITGC)	Audit Directly	Audit Directly	Audit Directly / Rely on third-party SOC report	Rely on third-party SOC report
Platform	Servers and operation systems	Audit Directly	Audit Directly	Rely on third-party SOC report	Rely on third-party SOC report
Infrastructure	Management console	Audit Directly	Audit Directly / Rely on third-party SOC report	Rely on third-party SOC report	Rely on third-party SOC report
Infrastructure	Data storage	Audit Directly	Rely on third-party SOC report	Rely on third-party SOC report	Rely on third-party SOC report
Infrastructure	Physical	Audit Directly	Rely on third-party SOC report	Rely on third-party SOC report	Rely on third-party SOC report

รายงาน SOC Report

SOC Report

- SOC – Service Organization Control Report
- รายงานผลการตรวจสอบที่จัดทำโดยผู้ตรวจสอบที่มีใบประกาศนียบัตรรับรอง CPA จากมาตรฐานสากล รับรองการควบคุมของผู้ให้บริการภายนอก (Service Organization หรือ CSP)

ประเภทของ SOC Report

SOC 1	
Scope: Internal Control over financial reporting	
SOC 1 Type 1	SOC 1 Type 2
Financial audit happens at a point in time	Financial audit happens over a period

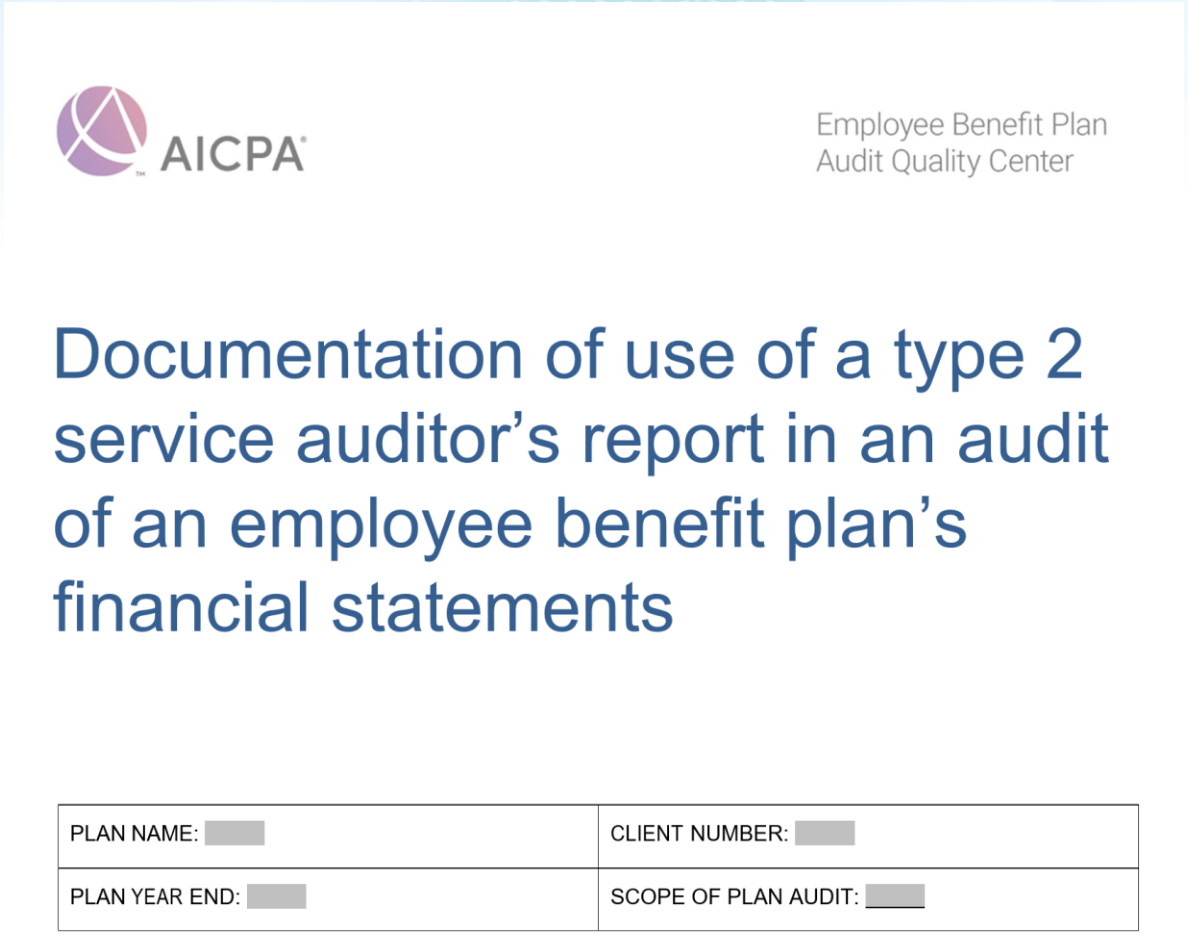
SOC 2	
Scope: **Security**, confidentiality, processing integrity, availability, privacy controls	
SOC 2 Type 1	SOC 2 Type 2
Compliance audit happens at a point in time	Compliance audit happens over a period

SOC 3
Scope: Same as SOC 2 (Summary – no detail)
SOC 3 Type 2 (Only type 2)
Compliance audit happens over a period (Summary)

แนวทางการสอบทาน SOC1 Type 2 Report

1. สอบทานขอบเขตการตรวจสอบ (ระบบงานและการควบคุม)
2. สอบทานระยะเวลาของการสุ่มตรวจสอบ
3. ประเมินความน่าเชื่อถือของผู้ตรวจสอบ
4. สอบทาน control objectives
5. สอบทานประเด็นที่ตรวจพบ (Deviation) และ การตอบสนอง (response)

ตัวอย่าง SOC 1 Type 2 Report



AICPA

Employee Benefit Plan
Audit Quality Center

Documentation of use of a type 2 service auditor's report in an audit of an employee benefit plan's financial statements

PLAN NAME:	CLIENT NUMBER:
PLAN YEAR END:	SCOPE OF PLAN AUDIT:

Ref: https://www.aicpa.org/resources/download/documenting-use-of-soc-1-report-in-an-employee-benefit-plan-audit

ตัวอย่าง SOC 1 Type 2 Report

Section I – Type 2 SOC 1 report general information

NAME OF SERVICE ORGANIZATION
NAME OF SERVICE AUDITOR
SERVICES PROVIDED BY THE SERVICE ORGANIZATION
LOCATIONS COVERED (IF APPLICABLE)
PERIOD COVERED BY THE TYPE 2 SOC 1 REPORT

Section II – Service auditor's opinion

What type of opinion did the service auditor express in the type 2 SOC 1 report?

_____ Unmodified

_____ Modified

If modified, document the nature of the modification(s), and any potential effect it may have on the risk of a material misstatement in the employee benefit plan's financial statements in the box provided below. Note: A modification may affect a single control objective (e.g., controls related to enrollment) or may affect several control objectives (e.g., IT general controls over logical access).

ตัวอย่าง SOC 1 Type 2 Report – (ต่อ)

Section III – Period covered by the type 2 SOC 1 report

Does the type 2 SOC 1 report cover the period covered by the plan's financial statements that are being audited?

_____ Yes (skip to Section IV)

_____ No

If the type 2 SOC 1 report does not cover a significant portion of the period covered by the plan's financial statements, was evidence about the operating effectiveness of controls obtained for the period that is not covered by the type 2 SOC 1 report by performing additional procedures? Examples of procedures that may be performed include:

- Making inquiries of the service organization about any major changes in the controls or processes, any noted issues, or any changes in programs or software at the service organization since the period covered by the service type 2 SOC 1 report.

  (Note: Some service organizations provide a "bridge letter" that addresses the period from the date of the service auditor's report through the most recent calendar year end.)

  Name of service organization representative contacted: _____

  Telephone number: _____

  Date contacted: _____

  Contacted by: _____

  Results: _____

- Reviewing documentation and correspondence issued by the service organization to management regarding changes to the programs, software, or controls or any noted issues.

- Obtaining additional audit evidence regarding the operating effectiveness of controls at the service organization for the portion of the period that is not covered by the type 2 SOC 1 report. If the plan auditor believes it is necessary, he or she may request that the user organization (plan) contact the service organization to request that the service auditor perform agreed-upon procedures at the service organization or the plan auditor may perform such procedures.

Conclusion:

Document the plan auditor's conclusion and any procedures performed, as applicable, and include any supporting documentation.

ตัวอย่าง SOC 1 Type 2 Report – (ต่อ)

Section IV – Service auditor's professional reputation

If the plan auditor is unfamiliar with or has no experience with the service auditor that issued the type 2 SOC 1 report, the plan auditor should perform procedures concerning the service auditor's professional reputation. Examples of procedures could include reviewing on-line sources of such information such as the Public Company Accounting Oversight Board's (PCAOB) website, which includes registration listings and inspection reports; the AICPA's website from which peer review reports and peer review acceptance letters can be accessed; and the website of the applicable state accountancy board. If no information can be found, document that fact, and determine the effect on the audit.

Was the service auditor's report prepared by a CPA firm with whom the plan auditor is familiar?

_____ Yes (skip to Section V)

_____ No

Document procedures performed and include any supporting documentation.

ตัวอย่าง SOC 1 Type 2 Report – (ต่อ)

Section V – Use of subservice organizations/carve-outs

Did the service organization outsource any functions relevant to the plan's internal control over financial reporting to another service organization (a subservice organization), and was the subservice organization carved out of the type 2 SOC 1 report?

_____ Yes

_____ No (skip to Section VI)

If yes, in the table below, list the names of the subservice organizations and the functions performed by the subservice organizations identified in the service auditor's type 2 SOC 1 report (and also in the description of the service organization's systems). (If the service auditor's report uses the carve-out method, the functions performed by the service organizations will be provided but the names of the subservice organizations may not be provided.) If the functions performed by the subservice organization are significant and relevant to the plan's internal control over financial reporting, the plan auditor may consider obtaining additional information about the subservice organization's controls. Such information may be available from user manuals, system overviews, technical manuals, the contract between the plan and the service organization, and reports on the subservice organization's controls, prepared by other service auditors, internal auditors, or a regulatory authority.

Complete column 3 to document or reference work performed to address the carved-out subservice organization(s). If the controls and functions performed by the subservice organization are not deemed relevant or significant to the plan's internal control over financial reporting, indicate N/A.

Name of subservice organization	Functions performed	Work performed to address carved-out subservice organization

ตัวอย่าง SOC 1 Type 2 Report – (ต่อ)

Section VI – Identification of control objectives and deviations noted

In this section, the plan auditor will begin to note the control objectives to determine what is present and what is not, and any noted deviations identified in the results of tests of controls that may affect the nature, timing and extent of audit procedures in an employee benefit plan audit. List below the control objectives included in the description of the service organization's system.

Control objectives included in the service organization's description of its system		Were deviations noted in the service auditor's description of tests of controls and results?		Page(s) #(s) in service organization's description or service auditor's description of tests of controls where control objective is located
Controls provide reasonable assurance that:		Yes*	No	
1.				
2.				

* For any yes answers, complete the table below.

In the table below, summarize the service organization's and plan auditor's response (if any) to any deviations identified by the service auditor in the description of tests of controls and results. *Note: Deviations in the results of tests of controls should be considered individually and in the aggregate to determine their effect, if any, on audit procedures to be performed.*

Control objective # (from table above)	Deviation(s) noted	Service organization's response included in the description of the service organization's system (such responses are not covered by the service auditor's opinion)	Plan auditor's response (see note below)

ตัวอย่าง SOC 1 Type 2 Report – (ต่อ)

Section VII – Complementary user entity controls

Summarize any complementary user entity control considerations identified in the service organization's description of its system.

No.	Complementary user entity control considerations identified in the service organization's description	Are the complementary user entity control considerations identified in the service organization's description relevant to the plan? If no, document below. If Yes, document or reference work performed to ensure complimentary user entity controls are in place	Work paper reference (see note below)
1.			
2.			
3.			

ตัวอย่าง SOC 1 Type 2 Report – (ต่อ)

Section VIII – Documentation of evaluation of the control objectives

If the type 2 SOC 1 report covers only the payroll process, skip Section VIII and go to Section IX.

In the following section, the reviewer or plan auditor can begin to evaluate whether the service organization's description of its system contains controls and control objectives relevant to the assertions included in the employee benefit plan's financial statements. (These are documented in columns #1 and #2 in the table below). In addition, the plan auditor will need to evaluate whether the tests of controls performed by the service auditor and the results of those tests provide sufficient appropriate evidence of the operating effectiveness of the controls to support the auditor's risk assessment.

The plan auditor should consider the following factors in making that evaluation:

- The nature, timing, and extent of the testing. For example, when testing controls, the service auditor should perform procedures in addition to inquiry, as required by related risk assessment standards
- Results of the tests of controls (e.g., any noted deviations)

Evaluation of the Control Objectives

Page # in the service organization's description of its system or service auditor's tests of controls where control objective is listed (from Section VI)	Control objective as listed in the description (from Section VI)	Does the description of the controls and the control objectives enable the plan auditor to evaluate the design and confirm the implementation of relevant controls and assess risk? (Yes/No)	Do the tests of operating effectiveness and results of those tests support the achievement of the stated control objective? (Yes/No) Note: Consider the effect of any deviations identified in the table above in Section VI	Reference from Section VII to complementary user entity controls identified in the description that are in place to support the plan auditor's risk assessment
IT General Controls/Control Objectives – Logical Access and Program Change Management				
Controls/Control Objectives Related to New Plan Set-up – Plan Provisions				

ตัวอย่าง SOC 1 Type 2 Report – (ต่อ)

Section IX – Payroll processing service organizations

Most large payroll processors provide a type 1 or type 2 report but such reports vary widely as to what services are covered. In addition, some payroll processors issue several reports that cover different locations, services or markets. Plan sponsors may contract with different payroll processors to provide different services. Plan sponsors are expected by the payroll processors to have controls in place to ensure accurate input and submission of data to the payroll processors (complementary user entity controls). Once the plan auditor has obtained the proper type 2 reports, the plan auditor can complete the following sections.

Documentation of the Evaluation of Payroll Reports

In the following section, the reviewer or plan auditor can begin to evaluate whether the report contains controls and control objectives relevant to the assertions included in the employee benefit plans financial statements. (These are documented in columns #1 and #2 in the table below). In addition, the plan auditor will need to evaluate whether the tests of controls performed by the service auditor and the results of those tests provide sufficient appropriate evidence of the operating effectiveness of the controls to support the auditor's risk assessment. The auditor should consider the following factors in making that evaluation:

- The nature, timing and extent of the testing. For example, when testing controls, the service auditor should perform procedures in addition to inquiry, as required by related risk assessment standards
- Results of the tests of controls (e.g., any noted deviations?)

Evaluation of the Control Objectives (Continued)

Page # in the service organization's description or service auditor's description of tests of controls where control objective is listed (from Section VI)	Control objective as listed in the description (from Section VI)	Does the description of the controls and the control objectives enable the plan auditor to evaluate the design and confirm the implementation of relevant controls and assess risk? (Yes/No)	Do the tests of operating effectiveness and results of those tests support the achievement of the stated control objective? (Yes/No) Note: Consider the effect of any deviations identified in the table above in Section VI	Reference from Section VII to complementary user entity controls identified in the description that are in place to support the plan auditor's risk assessment.
Controls/Control Objectives Related to Set-up of New Employees (demographic data, pay rates, withholding amounts)				

ตัวอย่าง SOC 1 Type 2 Report – (ต่อ)

Section X – Conclusion

Has the user auditor obtained a sufficient understanding of the control objectives and related controls at the service organization that is relevant to the plan's internal control over financial reporting in order to assess the risks of material misstatements and to design the nature, timing and extent of further audit procedures?

_____ Yes

_____ No

Note: If the plan auditor concludes that information is not available to obtain a sufficient understanding to assess the risks of material misstatement, he or she may consider contacting the service organization to obtain specific information or request that a service auditor be engaged to perform procedures that will provide the necessary information, or the plan auditor may visit the service organization and perform such procedures.

Include any additional comments.

_____

Prepared by: _____ Date: _____

Reviewed by: _____ Date: _____

กรณีตัวอย่าง

- Q: กรณีไม่มี SOC 1 Type 2 Report?
  - ให้ดำเนินการตรวจสอบเอง หากไม่สามารถให้เปลี่ยนแนวทางการตรวจสอบโดยไม่ Rely on การควบคุมของ Cloud
- Q: กรณีพบประเด็นในรายงาน SOC 1 Type 2
  - ให้ดำเนินการประเมินความเสี่ยงและผลกระทบ รวมถึงวางแผนการตรวจสอบเพิ่มเติมในส่วนของบริษัทเพื่อปิดความเสี่ยงดังกล่าว
- Q: กรณี Period ของรายงานไม่ตรง
  - ดูว่า Period ที่ขาดหายนั้น หายไปแบบมีสาระสำคัญหรือไม่
  - ดูว่า Auditor มีการจัดทำ Additional Procedure (Follow up) หรือไม่
  - ดูว่า Service Organization มีจัดทำ Bridge Letter หรือไม่
- Q: กรณีไม่มี SOC 1 Type 2 Report ใช้ ISO27001 ได้ไหม?
  - ISO27001 เป็นรายงานด้านความปลอดภัยของข้อมูล ไม่สามารถนำมาใช้ได้

มาตรฐานที่เกี่ยวข้อง

- TSA402 มาตรฐานการสอบบัญชี รหัส 402
  - ข้อพิจารณาในกรณีที่กิจการใช้บริการขององค์กรอื่น
- TSAE3402 มาตรฐานงานที่ให้ความเชื่อมั่น รหัส 3402
  - รายงานที่ให้ความเชื่อมั่นต่อการควบคุมขององค์กรที่ให้บริการ

ตรวจสอบการควบคุมของบริษัทที่ใช้ Cloud

เมื่อบริษัทใช้ Cloud ควรมีการควบคุมอย่างไร

การกำกับดูแล และจัดการความเสี่ยง

- นโยบายการกำกับดูแลผู้ให้บริการภายนอก และ การใช้งาน Cloud
- การประเมินความเสี่ยงและความจำเป็นในการใช้บริการ

การคัดเลือก

- กำหนดเกณฑ์การคัดเลือก
- กระบวนการคัดเลือก

การจัดทำสัญญา

- การกำหนด Service Level Agreement ในสัญญา
- การประเมินความเสี่ยงทั้ง 3 ด้าน
  - Confidentiality
  - Integrity
  - Availability
- ความสามารถในการตรวจสอบผู้ให้บริการ

การติดตามและประเมิน

- กระบวนติดตามประสิทธิภาพการให้บริการ
- การประเมินประสิทธิภาพการให้บริการ

บทสรุป

1. การแบ่งแยกการควบคุมที่บริหารจัดการระหว่างบริษัท และ CSP เพื่อวางแผนตรวจสอบ
2. ตรวจสอบการควบคุมของ CSP
   a. สอบทาน SOC Report (ถ้ามี) ดูความเหมาะสมพอเพียงของรายงาน (หากไม่เพียงพอให้ทำข้อ 2)
   b. สอบทานการควบคุมที่ผู้ให้บริการ Cloud (CSP) โดยผู้ตรวจสอบเอง โดยประสานงานผ่านบริษัทฯ
3. สอบทาน SOC 1 Type 2 Report
   a. สอบทานขอบเขตการตรวจสอบ (ระบบงานและการควบคุม)
   b. สอบทานระยะเวลาของการสุ่มตรวจสอบ
   c. ประเมินความน่าเชื่อถือของผู้ตรวจสอบ
   d. สอบทาน control objectives
   e. สอบทานประเด็นที่ตรวจพบ (Deviation) และ การตอบสนอง (response)
4. สอบทานการควบคุมฝั่งบริษัท

THANK YOU

https://www.tfac.or.th

@TFAC.FAMILY

tfac@tfac.or.th

https://www.facebook.com/TFAC.FAMILY

https:// www.youtube.com/TFACFamily

02 685 2500