สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์
Federation of Accounting Professions
Under the Royal Patronage of His Majesty the King

บทที่
5

ความเสี่ยง การควบคุม และการตรวจสอบการใช้เทคโนโลยีสมัยใหม่

(เอกสารประกอบการเตรียมตัวเป็นผู้สอบบัญชีรับอนุญาต)

โดย พิรุฬน์ กิตติเดชปรีชา
วราลี วัฒนวิบูลย์
เสาวนีย์ เสตเสถียร
คณะผู้ทรงคุณวุฒิเกี่ยวกับการทดสอบการปฏิบัติงานสอบบัญชี
ด้านการสอบบัญชีเนื้อหาการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์
สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

บทที่ 5
เรื่อง ความเสี่ยง การควบคุม และการตรวจสอบการใช้เทคโนโลยีสมัยใหม่

โดย พิรุฬน์ กิตติเดชปรีชา
วราลี วัฒนวิบูลย์
เสาวนีย์ เสตเสถียร
คณะผู้ทรงคุณวุฒิเกี่ยวกับการทดสอบการปฏิบัติงานสอบบัญชี
ด้านวการสอบบัญชีเนื้อหาการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์
สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

สารบัญบท

2. วัตถุประสงค์ในการศึกษา

เมื่อได้ศึกษาเนื้อหาของบทนี้แล้ว ผู้ศึกษาควรมีความเข้าใจถึง

1. ภาพรวมของเทคโนโลยีสมัยใหม่ที่กิจการอาจจะนำมาใช้
2. ความเสี่ยงที่อาจจะเกิดขึ้นจากการใช้งานเทคโนโลยีสมัยใหม่ต่อข้อมูลทางการเงิน
3. การควบคุมเบื้องต้นที่กิจการควรจะมีในกรณีที่กิจการใช้งานเทคโนโลยีสมัยใหม่เพื่อให้ข้อมูลทางการเงินมีความถูกต้องครบถ้วน
4. แนวทางการตรวจสอบเบื้องต้นในกรณีที่กิจการใช้เทคโนโลยีสมัยใหม่บันทึกรายการที่เกี่ยวข้องกับข้อมูลทางการเงิน

3. คำนำ

ในปัจจุบัน เทคโนโลยีมีความก้าวหน้าอย่างรวดเร็วและมีผลกระทบต่อทั้งการทำงานและการใช้ชีวิตประจำวันเป็นอย่างมาก การนำเทคโนโลยีมาใช้ในองค์กรกลายเป็นสิ่งที่จำเป็นในการดำเนินธุรกิจและช่วยสร้างความได้เปรียบเหนือคู่แข่ง หนึ่งในเทคโนโลยีที่เป็นที่นิยมและถูกนำมาใช้กันมากที่สุดในยุคปัจจุบัน คือ Cloud Computing เหตุผลที่ทำให้เทคโนโลยีดังกล่าวเป็นที่นิยมและยอมรับกันอย่างแพร่หลาย คือ การช่วยลดต้นทุนด้านเทคโนโลยี และเพิ่มประสิทธิภาพในการดำเนินธุรกิจ รวมถึง มีความยืดหยุ่นและรองรับการขยายตัวทางธุรกิจ อย่างไรก็ตาม การนำเทคโนโลยีดังกล่าวมาใช้งานมาพร้อมกับความเสี่ยงที่ผู้ประกอบธุรกิจต้องเผชิญ เช่น ความปลอดภัยของข้อมูลที่จัดเก็บ ความน่าเชื่อถือของผู้ให้บริการ Cloud Computing เป็นต้น ดังนั้น ผู้สอบบัญชีจึงมีความจำเป็นที่ต้องเข้าใจในเทคโนโลยี Cloud Computing เพื่อใช้ในการวางแผนและกำหนดวิธีการตรวจสอบงบการเงินของกิจการที่ใช้เทคโนโลยี Cloud Computing ในการบันทึกรายการและจัดทำรายงานทางการเงิน

เนื้อหาในส่วนนี้จึงเป็นการนำเสนอภาพรวมของเทคโนโลยี Cloud Computing ความเสี่ยงที่อาจเกิดขึ้น การควบคุมเบื้องต้นที่กิจการควรจัดให้มี และแนวการตรวจสอบเบื้องต้น เพื่อให้ผู้สอบบัญชีได้ใช้เป็นแนวทางในการวางแผนและกำหนดวิธีการตรวจสอบบัญชีในกรณีที่กิจการใช้เทคโนโลยี Cloud Computing ในการบันทึกรายการและจัดทำรายงานทางการเงิน

ภาพรวมของ Cloud Computing

Cloud Computing คือ การนำระบบสารสนเทศมาใช้ร่วมกันผ่านระบบเครือข่าย เพื่อประมวลผลตามความต้องการของผู้ใช้งาน โดยผู้ใช้งานไม่ต้องจัดหาฮาร์ดแวร์ หรือซอฟต์แวร์มาเอง แต่ใช้บริการจากผู้ให้บริการ (Cloud Service Provider: CSP) ผ่านทางระบบเครือข่าย สามารถแบ่งตามประเภทของการให้บริการ และรูปแบบการนำไปใช้งานได้ดังต่อไปนี้

4.1 ประเภทของการให้บริการ (Service Models)

1. Infrastructure-as-a-Service (IaaS) คือ การให้บริการโครงสร้างพื้นฐาน เช่น หน่วยประมวลผล (CPU) หน่วยความจำ (RAM) พื้นที่จัดเก็บข้อมูล ระบบเครือข่าย และเครื่องเสมือน (Virtual) เป็นต้น ผู้ใช้บริการสามารถบริหารจัดการ พัฒนา และเปลี่ยนแปลงแก้ไขแอปพลิเคชันได้เอง ดังนั้นผู้ใช้บริการยังคงต้องมีทรัพยากรบุคคลในด้านเทคโนโลยีสารสนเทศเพื่อใช้ในการบริหารจัดการระบบ ได้แก่ ผู้พัฒนาโปรแกรม (Developer) ผู้ดูแลระบบงาน (System Administrator) และผู้ดูแลฐานข้อมูล (Database Administrator) เช่นเดิม
2. Platform-as-a-Service (PaaS) คือ การให้บริการแพลตฟอร์ม เช่น ระบบปฏิบัติการ ระบบฐานข้อมูล และเครื่องมือที่ใช้ในการพัฒนาแอปพลิเคชัน เป็นต้น โดยผู้ใช้บริการสามารถพัฒนาและเปลี่ยนแปลงแก้ไขแอปพลิเคชันภายใต้ข้อจำกัดของแพลตฟอร์ม ดังนั้นผู้ใช้บริการยังคงต้องมี ผู้พัฒนาโปรแกรม (Developer) เพื่อพัฒนาและเปลี่ยนแปลงแก้ไขแอปพลิเคชัน แต่ไม่จำเป็นต้องมีผู้ดูแลระบบงาน และผู้ดูแลฐานข้อมูล เนื่องจากผู้ให้บริการจะเป็นผู้จัดหาบุคลากรมาดูแลแทน
3. Software-as-a-Service (SaaS) คือ การให้บริการซอฟต์แวร์ที่ผู้ใช้บริการเป็นผู้ใช้งานของแอปพลิเคชันตามสิทธิที่ผู้ให้บริการกำหนดไว้เท่านั้น ไม่สามารถเปลี่ยนแปลงแก้ไขแอปพลิเคชันได้เอง โดยผู้ใช้บริการเข้าใช้งานแอปพลิเคชันได้ผ่านอุปกรณ์ของผู้ใช้บริการ

4.2 บทบาทหน้าที่ของผู้เกี่ยวข้องและขอบเขตการตรวจสอบ Cloud Computing

บทบาทหน้าที่ของผู้เกี่ยวข้องและขอบเขตการตรวจสอบแบ่งตามประเภทการให้บริการ Cloud Computing โดยแยกตามองค์ประกอบเทคโนโลยีสารสนเทศ ดังรายละเอียดที่แสดงในตารางที่ 1.1 และตาราง 1.2 ดังนี้

ตารางที่ 1.1 บทบาทหน้าที่ของผู้เกี่ยวข้องตามประเภทการให้บริการ Cloud Computing

องค์ประกอบเทคโนโลยีสารสนเทศ	คำอธิบาย	ประเภทการให้บริการ		
		IaaS	PaaS	SaaS
User Access	สิทธิการเข้าถึงเมนูของผู้ใช้งาน	ผู้ใช้บริการ	ผู้ใช้บริการ	ผู้ใช้บริการ
Data	ข้อมูลสารสนเทศของกิจการ	ผู้ใช้บริการ	ผู้ใช้บริการ	CSP
Application Configuration	การบริหารจัดการ และเปลี่ยนแปลงแก้ไขโปรแกรมหรือชุดคำสั่ง	ผู้ใช้บริการ	ผู้ใช้บริการ	CSP
Middleware	ซอฟต์แวร์ที่ทำหน้าที่เป็นตัวกลางที่เชื่อมต่อการทำงานระหว่างระบบปฏิบัติการ (Operating System) กับ ระบบงาน (Application)	ผู้ใช้บริการ	CSP	CSP
Operating System	ระบบปฏิบัติการ เช่น Windows, Linux	ผู้ใช้บริการ	CSP	CSP
Storage	พื้นที่ในการจัดเก็บข้อมูล	CSP	CSP	CSP
Network	ระบบเครือข่าย	CSP	CSP	CSP
Physical	เครื่องแม่ข่าย (Server) ห้อง/ศูนย์คอมพิวเตอร์	CSP	CSP	CSP

* CSP (Cloud Service Provider)

ตารางที่ 1.2 ขอบเขตการตรวจสอบตามประเภทการใช้บริการ Cloud Computing

องค์ประกอบเทคโนโลยีสารสนเทศ	คำอธิบาย	ประเภทการให้บริการ		
		IaaS	PaaS	SaaS
User Access	สิทธิการเข้าถึงเมนูของผู้ใช้งาน	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (Access Control)	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (Access Control)	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (Access Control)
Data	ข้อมูลสารสนเทศของกิจการ	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (Data Security)	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (Data Security)	**ตรวจสอบ SOC report และสัญญาการให้บริการ**
Application Configuration	การบริหารจัดการ และเปลี่ยนแปลงแก้ไขโปรแกรมหรือชุดคำสั่ง	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (System Development Methodology and Program Change Management)	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (System Development Methodology and Program Change Management)	**ตรวจสอบ SOC Report และสัญญาการให้บริการ**
Middleware	ซอฟต์แวร์ที่ทำหน้าที่เป็นตัวกลางที่เชื่อมต่อการทำงานระหว่างระบบปฏิบัติการ (Operating System) กับ ระบบงาน (Application)	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (Access Control)	**ตรวจสอบ SOC Report และสัญญาการให้บริการ**	**ตรวจสอบ SOC Report และสัญญาการให้บริการ**
Operating System	ระบบปฏิบัติการ เช่น Windows, Linux	ตรวจสอบ ITGC ของผู้ใช้บริการโดยตรง (Access Control)	**ตรวจสอบ SOC Report และสัญญาการให้บริการ**	**ตรวจสอบ SOC Report และสัญญาการให้บริการ**
Storage	พื้นที่ในการจัดเก็บข้อมูล	**ตรวจสอบ SOC report และสัญญาการให้บริการ**	**ตรวจสอบ SOC report และสัญญาการให้บริการ**	**ตรวจสอบ SOC report และสัญญาการให้บริการ**
Network	ระบบเครือข่าย	**ตรวจสอบ SOC report และสัญญาการให้บริการ**	**ตรวจสอบ SOC report และสัญญาการให้บริการ**	**ตรวจสอบ SOC report และสัญญาการให้บริการ**
Physical	เครื่องแม่ข่าย (Server) ห้อง/ศูนย์คอมพิวเตอร์	**ตรวจสอบ SOC report และสัญญาการให้บริการ**	**ตรวจสอบ SOC report และสัญญาการให้บริการ**	**ตรวจสอบ SOC Report และสัญญาการให้บริการ**

SOC Report (Service Organization Control Report) ในที่นี้หมายถึง SOC1 Type 2 Report (โปรดอ่านรายละเอียดเพิ่มเติมในหัวข้อ การประเมินและตรวจสอบสารสนเทศบน Cloud Computing)

ITGC หมายถึง Information Technology General Control การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

4.3 รูปแบบการนำไปใช้งาน (Deployment Models)

1. Private Cloud (On-Premises or Internal) คือ ระบบ Cloud Computing ที่เปิดให้ใช้งานได้เฉพาะหน่วยงานภายในกิจการเดียวกัน มีการรักษาความปลอดภัย และความเป็นส่วนตัวของข้อมูลสูง เพราะข้อมูลถูกจัดเก็บบนเครื่องแม่ข่าย หรือศูนย์ข้อมูล (Data Center) ส่วนตัว

2. Community Cloud คือ ระบบ Cloud Computing ที่ใช้งานร่วมกัน โดยกลุ่มจากกิจการต่าง ๆ ที่มีจุดมุ่งหมายและความต้องการใช้งานแบบเดียวกัน เช่น สถาบันการศึกษา หรือกลุ่มธุรกิจ

3. Public Cloud (Off-Premises or External) คือ ระบบ Cloud Computing ที่เปิดให้ใช้งานผ่านระบบเครือข่ายสาธารณะเพื่อให้บริษัท กิจการ หรือบุคคลทั่วไปเข้ามาใช้บริการ และเก็บค่าใช้บริการในรูปแบบต่าง ๆ เช่น รายเดือน รายปี ตามปริมาณการใช้งาน หรือตามจำนวนผู้ใช้งาน เป็นต้น

4. Hybrid Cloud (Integrated Public and Private Services)คือ ระบบ Cloud Computing ที่ประกอบด้วยรูปแบบการนำไปใช้งานตั้งแต่ 2 รูปแบบขึ้นไปเพื่อลดข้อเสียของการเลือกใช้งาน Cloud Computing แต่ละรูปแบบ

5. ความเสี่ยงจากการใช้บริการและการควบคุมบน Cloud Computing

การนำ Cloud Computing มาใช้ในกิจการเป็นการนำระบบสารสนเทศมาใช้ร่วมกันผ่านระบบเครือข่ายทำให้มีผลกระทบต่อสภาพแวดล้อมทางเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศ ผู้สอบบัญชีควรทำความเข้าใจการใช้งาน Cloud Computing ของกิจการ และระบุความเสี่ยงที่อาจเกิดขึ้นรวมถึงผลกระทบต่อการตรวจสอบบัญชีจากการใช้งานเทคโนโลยีดังกล่าว ดังนั้น เพื่อให้มั่นใจว่ากิจการได้จัดให้มีการควบคุมอย่างเพียงพอให้สอดคล้องกับความเสี่ยงและข้อกำหนด หลักเกณฑ์ และ/หรือแนวปฏิบัติที่เกี่ยวข้อง ในส่วนนี้จะกล่าวถึงตัวอย่างความเสี่ยงและการควบคุมที่ควรพิจารณาในแต่ละหัวข้อ โดยมีรายละเอียดดังนี้

ความเสี่ยง	การควบคุม
1. นโยบายและขั้นตอนการปฏิบัติงานการใช้งานระบบ Cloud Computing	
การใช้งาน Cloud Computing ไม่สอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ของกิจการ	มีการประเมินประโยชน์ทางธุรกิจในการใช้งาน Cloud Computing รวมถึงผู้บริหารระดับสูงสนับสนุนการนำ Cloud Computing มาใช้งานเพื่อบรรลุวัตถุประสงค์เชิงกลยุทธ์ของกิจการ
ไม่ได้เลือกผู้ให้บริการที่ตรงกับประเภทงานที่จะใช้บริการ	ผู้ให้บริการมีความสามารถเชิงเทคนิคในการสนับสนุนการให้บริการ Cloud Computing และได้รับการตรวจสอบโดยละเอียดอย่างเหมาะสมจากกิจการ
ไม่มีกรอบการกำกับดูแลที่เพียงพอในการกำกับดูแลเทคโนโลยี Cloud Computing	มีการกำหนดและอนุมัติกรอบการกำกับดูแลการนำเทคโนโลยี Cloud Computing มาใช้งาน
การให้บริการของผู้ให้บริการ Cloud Computing ไม่เป็นไปตามข้อตกลง	มีกระบวนการติดตามการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ
2. การบริหารจัดการ การเข้าถึงข้อมูลและการพิสูจน์ตัวตน (Identity and Access Management)	
มีการเข้าถึงระบบ Cloud Computing โดยผู้ไม่ได้รับอนุญาต	มีการควบคุมการเข้าถึงระบบ Cloud Computing
มีการแก้ไขโดยไม่ได้รับอนุญาตบนระบบ Cloud Computing	มีการควบคุมการเปลี่ยนแปลง และ กระบวนการการติดตามการแก้ไขระบบ Cloud Computing
การนำระบบ Cloud Computing ไปใช้ในระบบงานจริง (Deployment) ไม่ได้รับการจัดการอย่างเหมาะสมทำให้ส่งผลกระทบต่อการใช้งานของกิจการ	มีแผนการนำระบบ Cloud Computing ไปใช้ในระบบงานจริง (Deployment Plan) ครบถ้วนตามที่กำหนดในข้อกำหนดความต้องการของระบบ

ความเสี่ยง	การควบคุม
3. การบริหารจัดการเหตุการณ์ผิดปกติ (Incident Management)	
เหตุการณ์ที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศไม่ถูกจัดการอย่างเหมาะสม ทำให้ไม่สามารถตรวจจับหรือติดตามเหตุการณ์ได้อย่างทันท่วงที	มีการกำหนดบทบาทการรายงานเหตุการณ์ที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศจากผู้ให้บริการ Cloud Computing
กระบวนการจัดการการเปลี่ยนแปลงไม่สามารถช่วยลดผลกระทบของเหตุการณ์ไม่ปกติที่เกี่ยวข้องและส่งผลกระทบกับการดำเนินงานประจำวันได้	มีการออกแบบและใช้วิธีการและขั้นตอนมาตรฐานสำหรับในการจัดการการเปลี่ยนแปลงระบบ Cloud Computing ให้มีการดำเนินการอย่างมีประสิทธิภาพ
4. ความมั่นคงปลอดภัยของอุปกรณ์เครือข่าย (Network Perimeter Security)	
การเข้าถึงระบบ Cloud Computing ผ่านระบบเครือข่ายไม่มีความปลอดภัย	มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยระบบเครือข่ายเพื่อบริหารจัดการและควบคุมระบบเครือข่ายอย่างมั่นคงปลอดภัย รวมถึงมีการติดตั้งชุดปรับปรุงซอฟต์แวร์ (Patch) บนอุปกรณ์เครือข่ายอย่างสม่ำเสมอ
5. การเข้ารหัส (Cryptography)	
ข้อมูลที่รับส่งระหว่างเครือข่ายที่เชื่อมต่อกับระบบ Cloud Computing ไม่มีความปลอดภัยทำให้สามารถเข้าถึงหรือเปลี่ยนแปลงข้อมูลที่มีความสำคัญได้	มีการกำหนดนโยบายการใช้งานการควบคุมด้านการเข้ารหัสของระบบ Cloud Computing ที่สามารถป้องกันการเข้าถึงหรือเปลี่ยนแปลงข้อมูลที่มีความสำคัญได้
6. ความถูกต้องและปลอดภัยของข้อมูล (Data Security and Integrity)	
ระบบ Cloud Computing อาจไม่ได้รับการจัดสรรทรัพยากรได้อย่างเหมาะสม	มีการประเมินความเพียงพอของระบบ Cloud Computing อย่างสม่ำเสมอ
มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตบนระบบ Cloud Computing	มีการจัดชั้นความลับข้อมูล (Information Classification) และกำหนดมาตรการปกป้องและเข้าถึงข้อมูลในแต่ละชั้นความลับ
การนำระบบ Cloud Computing ไปใช้ในระบบงานจริง (Deployment) ไม่ได้รับการจัดการอย่างเหมาะสมทำให้ส่งผลกระทบต่อการใช้งานของกิจการ	มีแผนการนำระบบ Cloud Computing ไปใช้ในระบบงานจริง (Deployment Plan) ครบถ้วนตามที่กำหนดในข้อกำหนดความต้องการของระบบ
แผนความต่อเนื่องทางธุรกิจของกิจการไม่ได้รวมเอาองค์ประกอบที่เกี่ยวข้องกับการดำเนินงานที่ใช้เทคโนโลยี Cloud Computing มาใช้ในกิจการ	มีแผนความต่อเนื่องทางธุรกิจสำหรับการใช้งานเทคโนโลยี Cloud Computing
ระบบ Cloud Computing ไม่สามารถกู้คืนระบบได้อย่างทันท่วงทีในกรณีระบบขัดข้องและจำเป็นต้องกู้คืนระบบ	ข้อตกลงในการสำรองข้อมูลให้สอดคล้องกับนโยบายของกิจการรวมถึงมีการบันทึกเหตุการณ์ผิดปกติที่เกี่ยวข้องกับระบบ Cloud Computing
ในกรณียกเลิกการใช้บริการ Cloud Computing อาจทำให้กิจการไม่สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง	มีกระบวนการและระเบียบปฏิบัติในการยกเลิกการใช้บริการ Cloud Computing ที่ชัดเจน

ความเสี่ยง	การควบคุม
7. การบริหารจัดการช่องโหว่ความปลอดภัย (Vulnerability Management)	
ระบบ Cloud Computing ถูกจู่โจมจากบุคคลภายนอกเพื่อทำให้ระบบใช้งานไม่ได้หรือทำให้ข้อมูลสำคัญได้รับความเสียหาย	มีการประเมินช่องโหว่ของระบบ (Vulnerability Assessment) และทดสอบการเจาะระบบ (Penetration Test) กับระบบ Cloud Computing รวมถึงระบบงานที่มีความสำคัญที่เชื่อมต่อกับเครือข่ายภายนอก
8. การปฏิบัติตามข้อกำหนดทางกฎหมายที่เกี่ยวข้อง (Compliance)	
ไม่ได้พิจารณากรอบการกำกับดูแลหรือกฎหมายที่จำเป็นต้องปฏิบัติตามในการดำเนินธุรกิจของตน	มีการระบุและปฏิบัติตามกรอบภายนอกที่เกี่ยวข้อง มีการรายงานผลการประเมินการปฏิบัติตามข้อกำหนดต่อผู้มีหน้าที่กำกับดูแล
ระบบ Cloud Computing ที่ให้บริการอาจไม่ได้ปฏิบัติตามกฎหมาย	มีการพิจารณาและประเมินข้อกำหนดทางกฎหมายและมีมาตรการตรวจสอบด้านสิทธิและเงื่อนไขการใช้งานซอฟต์แวร์

6. การประเมินและตรวจสอบสารสนเทศบน Cloud Computing

วัตถุประสงค์ของการตรวจสอบ

1. ประเมินนโยบายและขั้นตอนการปฏิบัติงานการใช้งานระบบ Cloud Computing รวมถึงการนำไปปฏิบัติจริง
2. ประเมินการควบคุมภายในและการปฏิบัติตามข้อกำหนดทางกฎหมายที่เกี่ยวข้อง
3. ประเมินการดำเนินงานโดยผู้ให้บริการ หรือ Cloud Service Provider (CSP) ในด้านความมั่นคงปลอดภัยสารสนเทศ (Security) ความพร้อมใช้งานของการให้บริการ (Availability) และความบูรณภาพ (ถูกต้องครบถ้วน) ของข้อมูล (Integrity)

ถึงแม้ว่ากิจกรรมการบริหารงานด้านสารสนเทศของการใช้บริการ Cloud Computing นั้นจะมีการดำเนินงานโดยผู้ให้บริการ Cloud Computing แต่อย่างไรก็ตาม กิจการยังคงมีหน้าที่และความรับผิดชอบต่อกิจกรรมการบริหารด้านสารสนเทศ รวมถึงหน้าที่ในการควบคุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่อยู่นอกเหนือข้อตกลงการให้บริการ ดังนั้น กิจการจึงต้องประเมินและจัดให้มีการควบคุมการใช้งานระบบประมวลผลในส่วนที่รับผิดชอบให้สอดคล้องกับความเสี่ยงและข้อกำหนด หลักเกณฑ์ และ/หรือแนวปฏิบัติที่เกี่ยวข้อง (อ้างอิง ตารางบทบาทหน้าที่ของผู้เกี่ยวข้องตามประเภทการใช้บริการ Cloud Computing) นอกจากนี้กิจการควรให้ความสำคัญกับประสิทธิภาพการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ (IT General Control) ในหัวข้อ ดังต่อไปนี้

1. นโยบายและขั้นตอนการปฏิบัติงานการใช้งานระบบ Cloud Computing กิจการควรมีการจัดทำนโยบายการใช้งานระบบ Cloud Computing ที่ชัดเจนเป็นลายลักษณ์อักษร และได้รับการอนุมัติหรือเห็นชอบจากผู้บริหาร โดยนโยบายฯ ต้องประกอบไปด้วยหัวข้อที่สำคัญ ดังต่อไปนี้
   - การกำหนดประเภทงานที่จะใช้บริการ
   - ประเภทของการใช้งานระบบ Cloud Computing ที่สามารถใช้งานได้ เช่น Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) และ/หรือ Infrastructure-as-a-Service (IaaS) และรูปแบบการใช้บริการ เช่น Private, Public หรือ Hybrid
   - ประเภทของข้อมูล รวมถึงมาตราการและวิธีปฏิบัติในการรักษาความปลอดภัยของข้อมูลแต่ละประเภทตามชั้นความลับของข้อมูล
   - การประเมินความเสี่ยงและการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและความปลอดภัยด้านไซเบอร์จากการใช้งาน Cloud Computing
   - การประเมินและการคัดเลือกผู้ให้บริการ

- การจัดทำสัญญาและข้อตกลงการให้บริการ
- การติดตามและการรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นจากการให้บริการอย่างสม่ำเสมอ
- การตรวจสอบโดยผู้ตรวจสอบอิสระ
- บทบาทหน้าที่ความรับผิดชอบของเจ้าหน้าที่ผู้เกี่ยวข้อง
- การสื่อสารนโยบายฯ
- การทบทวนนโยบายฯ

2. การบริหารจัดการ การเข้าถึงข้อมูลและการพิสูจน์ตัวตน (Identity and Access Management) ตรวจสอบหัวข้อ ดังต่อไปนี้เป็นอย่างน้อย
   - การจัดการสิทธิกลุ่มผู้ใช้งานระบบงาน* หรือบริการบน Cloud Computing และลักษณะการใช้งานและบริการ
   - การบริหารจัดการสิทธิกลุ่มผู้ดูแลระบบ (Administrator) ที่มีสิทธิเข้าถึงและใช้งานระดับสูง*
   - การสอบทานสิทธิอย่างสม่ำเสมอ* (Periodic Review)
   - การแบ่งแยกหน้าที่งานของผู้พัฒนา กับผู้ Release Solution บน Platform Cloud Computing
   - กระบวนการพิสูจน์ตัวตนในการควบคุมการเข้าถึง* เช่น Multi-Factor Authentication, การเข้ารหัสโทเคน (Tokenization)
3. การบริหารจัดการเหตุการณ์ผิดปกติ (Incident Management) ตรวจสอบหัวข้อดังต่อไปนี้เป็นอย่างน้อย
   - ประเภทเหตุการณ์ที่ผู้ให้บริการต้องรายงานมายังกิจการ
   - ช่องทางติดต่อและผู้รับผิดชอบด้านปัญหาการใช้งาน และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ
   - การจัดเก็บบันทึกเหตุการณ์ ประเภทของเหตุการณ์ ระยะเวลาการจัดเก็บข้อมูล การป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล และหน้าที่ความรับผิดชอบในการวิเคราะห์เหตุการณ์
4. ความมั่นคงปลอดภัยของอุปกรณ์เครือข่าย (Network Perimeter Security) ตรวจสอบหัวข้อดังต่อไปนี้เป็นอย่างน้อย
   - การประมวลผลบนระบบเสมือน (Virtualization) ที่อาจมีผู้ใช้งานร่วมกันอยู่ภายใต้สภาพแวดล้อมเดียวกัน
   - การติดตามและติดตั้งชุดปรับปรุงซอฟต์แวร์ (Patch Management)
   - มาตรการการรักษาความมั่นคงปลอดภัยเครือข่าย*
   - การวิเคราะห์ข้อมูลและการเฝ้าระวังการโจมตีทางเครือข่าย
5. การเข้ารหัส (Cryptography) ตรวจสอบหัวข้อดังต่อไปนี้เป็นอย่างน้อย
   - ใช้เทคโนโลยีการเข้ารหัสที่สอดคล้องกับความเสี่ยงในกระบวนการรับส่งและจัดเก็บข้อมูลบนระบบ Cloud Computing ทั้งกรณีดำเนินการโดยกิจการ หรือดำเนินการโดยผู้ให้บริการ
   - การควบคุมและจัดการกุญแจการเข้ารหัส (Cryptographic Key) ที่มีการใช้งานบนระบบ Cloud Computing ให้เป็นไปตามนโยบายและบริหารจัดการกุญแจการเข้ารหัส
   - กรณีการบริหารจัดการกุญแจการเข้ารหัสโดยผู้ให้บริการ กิจการควรรวบรวมข้อมูลและแนวทางการจัดการกุญแจการเข้ารหัสที่อยู่ในความดูแลของผู้ให้บริการ ดังนี้
     - ประเภทของกุญแจการเข้ารหัส
     - กระบวนการบริหารจัดการกุญแจการเข้ารหัส ได้แก่ การสร้าง การแก้ไข เปลี่ยนแปลง การจัดเก็บ การเข้าถึง การยกเลิกและทำลายกุญแจการเข้ารหัส
   - กรณีการบริหารจัดการกุญแจการเข้ารหัสดำเนินการโดยผู้ประกอบการ กิจการไม่ควรได้รับสิทธิการเข้าถึง จัดเก็บ และบริหารจัดการกุญแจการเข้ารหัส

6. ความถูกต้องและปลอดภัยของข้อมูล (Data Security and Integrity) ตัวอย่างเช่น
   - ข้อมูลที่มีการจัดเก็บบนระบบ Cloud Computing ที่อาจมีการเข้าถึงและบริหารจัดการโดยบริษัทผู้ให้บริการ หรือ Cloud Service Provider (CSP)
   - ประเภทของสินทรัพย์สารสนเทศ (Assets) ที่มีการประมวลผล และบริหารจัดการบนสภาพแวดล้อมระบบ Cloud Computing ควรมีการจัดทำรายการสินทรัพย์สารสนเทศพร้อมรายละเอียด และมีการจัดชั้นความลับข้อมูลและระบุประเภท* (Label)
   - การสำรองข้อมูลและกู้คืนข้อมูล* เพื่อให้มั่นใจว่ากิจการสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง
   - พื้นที่และประเทศที่ผู้ให้บริการ Cloud Computing จัดเก็บข้อมูลและประมวลผล รวมถึงการจัดเก็บข้อมูลแบบชั่วคราว
   - ขั้นตอนการโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ กรณีมีการเปลี่ยนบริษัทผู้ให้บริการ หรือ Cloud Service Provider (CSP)
   - การจัดเก็บและทำลายข้อมูลเมื่อมีการยกเลิกหรือสิ้นสุดสัญญาการให้บริการ
7. การบริหารจัดการช่องโหว่ความปลอดภัย (Vulnerability Management)
8. การปฏิบัติตามข้อกำหนดทางกฎหมายที่เกี่ยวข้อง (Compliance) ตัวอย่างเช่น
   - พ.ร.บ. ข้อมูลส่วนบุคคล
   - พ.ร.บ ด้านความมั่นคงปลอดภัยด้านไซเบอร์
   - ข้อกำหนดหรือประกาศด้านความมั่นคงปลอดภัยด้านไซเบอร์ หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้องของหน่วยงานกำกับดูแลที่กิจการอยู่ภายใต้การกำกับ เช่น ธนาคารแห่งประทศไทย และ/หรือตลาดหลักทรัพย์แห่งประเทศไทย
   - กฎหมายและข้อบังคับของทั้งในและนอกประเทศ

สำหรับกิจกรรมด้านเทคโนโลยีสารสนเทศที่อยู่ภายใต้ความรับผิดชอบของผู้ให้บริการ Cloud Computing กิจการควรจัดให้มีการควบคุมและติดตามผลการดำเนินงานให้เป็นไปตามข้อตกลงการให้บริการ และสอดคล้องกับมาตรฐานสากลเพิ่มเติม ดังนี้

1. รายงานตรวจสอบโดยผู้ตรวจสอบอิสระด้านการควบคุมของกิจการที่ให้บริการ (Service Organization Control (SOC) Report) โดยพิจารณาถึงเรื่องดังต่อไปนี้เป็นอย่างน้อย
   - ประเภทของรายงาน เช่น SOC1 Type 2, SOC2, SOC3, SOC for Cyber Security เป็นต้น ซึ่งมีรายละเอียดที่แตกต่างกัน ดังนี้

	SOC1 Type 2 (TSAE3402)	SOC2 (TSAE3000)	SOC3	SOC for Cyber Security
สิ่งที่เน้น	รายงานที่ให้ความเชื่อมั่นต่อประสิทธิผลของการปฏิบัติตามการควบคุมเพื่อที่จะบรรลุวัตถุประสงค์ของการควบคุมที่ระบุไว้โดยกิจการที่ให้บริการ	รายงานการควบคุมที่เกี่ยวข้องกับความปลอดภัย (Security) ความพร้อมใช้งาน (Availability) การประมวลแบบบูรณาการ (Processing Integrity) ข้อมูลลับเฉพาะ (Confidentiality) และ/หรือ ความเป็นส่วนตัวของข้อมูล (Privacy)	รายงานการควบคุมที่เกี่ยวข้องกับความปลอดภัย (Security) ความพร้อมใช้งาน (Availability) การประมวลแบบบูรณาการ (Processing Integrity) ข้อมูลลับเฉพาะ (Confidentiality) และ/หรือ ความเป็นส่วนตัวของข้อมูล (Privacy)	รายงานโปรแกรมการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยด้านไซเบอร์และการประเมินประสิทธิภาพของการควบคุม

	SOC1 Type 2 (TSAE3402)	SOC2 (TSAE3000)	SOC3	SOC for Cyber Security
ประเภทของกระบวนการและระบบงาน	จำกัดกระบวนการและระบบงานที่ใช้ในการจัดทำรายงานทางการเงินของกิจการที่ใช้บริการ	สามารถเป็นกระบวนการหรือระบบงานใดก็ได้แล้วแต่ข้อตกลง	สามารถเป็นกระบวนการหรือระบบงานใดก็ได้แล้วแต่ข้อตกลง	โปรแกรมการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยด้านไซเบอร์ตามเกณฑ์คำอธิบาย
เกณฑ์	ออกแบบเพื่อให้ความเชื่อมั่นต่อประสิทธิผลของการควบคุม ณ กิจการผู้ให้บริการ ซึ่งเกี่ยวข้องกับการจัดทำรายงานทางการเงินของกิจการที่ใช้บริการ	ออกแบบเพื่อให้ความมั่นใจต่อลูกค้า คู่ค้าทางธุรกิจ (Business Partners) รวมถึงกิจการหรือบุคคลอื่นที่สนใจ (Interested Parties)	ออกแบบ เพื่อให้ความมั่นใจต่อลูกค้า คู่ค้าทางธุรกิจ (Business Partners) รวมถึงกิจการหรือบุคคลอื่นที่สนใจ (Interested Parties)	ออกแบบเพื่อให้ข้อมูลที่เป็นประโยชน์ต่อผู้ใช้งานทั่วไป เกี่ยวกับโปรแกรมการบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยด้านไซเบอร์ของกิจการ
ผู้ใช้งาน	กิจการที่ใช้บริการของผู้ให้บริการ หรือผู้สอบบัญชี	ลูกค้า คู่ค้าทางธุรกิจ (Business Partners) รวมถึงกิจการหรือบุคคลอื่นที่สนใจ (Interested Parties)	ลูกค้า คู่ค้าทางธุรกิจ (Business Partners) รวมถึงกิจการหรือบุคคลอื่นที่สนใจ (Interested Parties)	คณะกรรมการบริหาร และผู้บริหารของผู้ใช้งานทั่วไป ซึ่งการตัดสินใจมีผลต่อการประเมินการควบคุมภายในและโปรแกรมการบริหารจัดการความเสี่ยงความมั่นคง
การใช้รายงาน	มีข้อจำกัด	อาจจะมีข้อจำกัด	โดยทั่วไปแล้ว ไม่มีข้อจำกัด	เหมาะสำหรับการใช้โดยทั่วไป

หมายเหตุ: TSAE คือ มาตรฐานงานที่ให้ความเชื่อมั่น (Thai Standards on Assurance Engagements) ออกโดยสภาวิชาชีพบัญชีฯ

- ขอบเขตการตรวจสอบสอดคล้องกับมาตรการรักษาความปลอดภัยที่อยู่ในความรับผิดชอบของผู้ให้บริการ รวมถึงข้อกำหนดที่เป็นที่ยอมรับในสากล (Global Practice) และหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศและแนวปฏิบัติที่เกี่ยวข้อง
  - ขอบเขตระบบที่อยู่ภายใต้การตรวจสอบ
  - รายละเอียดวิธีการตรวจสอบ
  - ระยะเวลาที่ครอบคลุมในรายงานการตรวจสอบ
  - ผลการตรวจสอบและประเด็นสำคัญในผลการตรวจสอบ
  - ความสามารถและความน่าเชื่อถือของผู้ตรวจสอบอิสระ

2. รายงานการปฏิบัติตามระดับการให้บริการที่จัดเตรียมโดยผู้ให้บริการ เช่น ร้อยละของการให้บริการอย่างต่อเนื่อง ระยะเวลาการตอบสนองและแก้ไขปัญหาตามข้อกำหนด การปรับปรุงและติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่อง รายงานผลการสำรองข้อมูล เป็นต้น

4. บรรณานุกรม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562, พฤษภาคม). *ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์.*

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2562, พฤศจิกายน). *Cloud Computing Practice.*

KPMG. (2015). *How to Manage 5 Key Cloud Computing Risks.*

KPMG. (2022). *Cloud Security Controls Framework.*

KPMG. (2023). *Cloud Controls Assessment Framework.*

คณะผู้ทรงคุณวุฒิจัดทำคู่มือด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์

ศ.ดร.ศิริลักษณ์	โรจนกิจอำนวย	ประธานคณะทำงาน
ศ.ดร.นิตยา	วงศ์ภินันท์วัฒนา	คณะทำงาน
ดร.เยาวลักษณ์	ชาติบัญชาชัย	คณะทำงาน
นางปิยะพัชร์	อัศวจินดากรณ์	คณะทำงาน
นางสาวผุสดี	จันทะสุวันนะ	คณะทำงาน
นายพิรุฬน์	กิตติเดชปรีชา	คณะทำงาน
นางสาวรินรัตน์	ภาสเวคิน	คณะทำงาน
นางวราลี	วัฒนวิบูลย์	คณะทำงาน
นายวันชัย	พิทักษ์กรณ์	คณะทำงาน
นางเสาวนีย์	เสตเสถียร	คณะทำงาน
นายอธิษฐ์	ตระกูลเดช	คณะทำงาน

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

เลขที่ 133 ถนนสุขุมวิท 21 (อโศก) แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

0 2685 2500 โทรสาร 0 2685 2501

tfac@tfac.or.th www.tfac.or.th