สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์

การตรวจสอบระบบสารสนเทศ
Information systems audit

ฉบับพิมพ์ครั้งที่ 3 แก้ไขเพิ่มเติม

ศาสตราจารย์ ดร.นิตยา วงศ์ภินันท์วัฒนา

สารบัญ

คำนำ		**(8)**
บทที่ 1	**แนวทางในการตรวจสอบระบบสารสนเทศ**	**1**
	วัตถุประสงค์	1
	บทนำ	2
	ภาพรวมของการตรวจสอบระบบสารสนเทศ	3
	องค์ความรู้สำหรับผู้ตรวจสอบระบบสารสนเทศ	12
	การประเมินความเสี่ยง	15
	สรุป	30
	คำถามท้ายบท	31
ภาคผนวก	การเปรียบเทียบความแตกต่างระหว่างการตรวจสอบแบบดั้งเดิมและการตรวจสอบแบบใหม่	32
บทที่ 2	**เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ**	**33**
	วัตถุประสงค์	33
	บทนำ	34
	เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบหลังจากรายการเกิดขึ้นแล้ว	34
	เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบระหว่างการปฏิบัติงานจริง	45
	การตรวจสอบรหัสคำสั่ง	50
	เทคนิคการทำเหมืองข้อมูลเพื่อการตรวจสอบ	54
	เทคนิคการทดสอบการเจาะระบบ	56
	โปรแกรมสำเร็จรูปเพื่อใช้สนับสนุนการตรวจสอบ	61
	สรุป	69
	คำถามท้ายบท	70
ภาคผนวก 1	การใช้งานโปรแกรม ACL version 9 (educational edition)	72
ภาคผนวก 2	สรุปสาระสำคัญของโปรแกรม Microsoft Excel สำหรับงานบัญชีและการตรวจสอบ	86
ภาคผนวก 3	ตัวอย่างการจัดทำเงื่อนไขเพื่อสร้างเป็นข้อมูลทดสอบ	103
บทที่ 3	**การตรวจสอบการดำเนินงานของผู้บริหารระบบสารสนเทศ**	**108**
	วัตถุประสงค์	108
	บทนำ	109
	ความเสี่ยงและการควบคุมการดำเนินงานของผู้บริหารระบบสารสนเทศ	109
	แนวทางการตรวจสอบการดำเนินงานของผู้บริหารระบบสารสนเทศ	111

	สรุป	118
	คำถามท้ายบท	119
บทที่ 4	**การตรวจสอบด้านการปฏิบัติการระบบสารสนเทศ**	**121**
	วัตถุประสงค์	121
	บทนำ	122
	ความเสี่ยงและการควบคุมด้านการปฏิบัติการระบบสารสนเทศ	122
	แนวทางการตรวจสอบด้านการปฏิบัติการระบบสารสนเทศ	124
	สรุป	135
	คำถามท้ายบท	136
บทที่ 5	**การตรวจสอบระบบเครือข่ายคอมพิวเตอร์**	**139**
	วัตถุประสงค์	139
	บทนำ	140
	ความเสี่ยงและการควบคุมระบบเครือข่ายคอมพิวเตอร์	140
	แนวทางการตรวจสอบระบบเครือข่ายคอมพิวเตอร์	143
	สรุป	156
	คำถามท้ายบท	157
บทที่ 6	**การตรวจสอบระบบปฏิบัติการ**	**159**
	วัตถุประสงค์	159
	บทนำ	160
	ความเสี่ยงและการควบคุมระบบปฏิบัติการ	160
	แนวทางการตรวจสอบระบบปฏิบัติการ	162
	สรุป	170
	คำถามท้ายบท	171
บทที่ 7	**การตรวจสอบฐานข้อมูล**	**173**
	วัตถุประสงค์	173
	บทนำ	174
	ความเสี่ยงและการควบคุมฐานข้อมูล	174
	แนวทางการตรวจสอบฐานข้อมูล	176
	สรุป	191
	คำถามท้ายบท	192

บทที่ 8 การตรวจสอบโปรแกรมประยุกต์ **196**
วัตถุประสงค์ 196
บทนำ 197
ความเสี่ยงและการควบคุมโปรแกรมประยุกต์ 197
แนวทางการตรวจสอบโปรแกรมประยุกต์ 202
สรุป 215
คำถามท้ายบท 217
ภาคผนวก 1 การควบคุมการติดตั้งโปรแกรมประยุกต์ 219
ภาคผนวก 2 ตัวอย่างการใช้โปรแกรม ACL version 9 (educational edition) เพื่อตรวจสอบโปรแกรมประยุกต์ 221
ภาคผนวก 3 ตัวอย่างแบบสอบถามสำหรับตรวจสอบระบบ ERP 246

บทที่ 9 รายงานการตรวจสอบระบบสารสนเทศ **256**
วัตถุประสงค์ 256
บทนำ 257
การจัดทำรายงานการตรวจสอบระบบสารสนเทศ 257
สรุป 267
คำถามท้ายบท 268

บทที่ 10 เกมบทบาทการตรวจสอบระบบสารสนเทศ **270**
วัตถุประสงค์ 270
บทนำ 271
กระบวนการของเกมบทบาทการตรวจสอบระบบสารสนเทศ 271
ข้อมูลและเอกสารเบื้องต้นที่ใช้ประกอบกรณีศึกษา 272
สรุป 282
คำถามท้ายบท 283

บรรณานุกรม **284**
ดรรชนีคำสำคัญ **288**

คำนำ

หนังสือ*การตรวจสอบระบบสารสนเทศ*เล่มนี้ ได้รวบรวมความรู้เกี่ยวกับการตรวจสอบระบบสารสนเทศ จากประสบการณ์ของผู้เขียนด้านการตรวจสอบระบบสารสนเทศของธุรกิจขนาดใหญ่ การสอนและการศึกษาค้นคว้าทางด้านวิชาการของระบบสารสนเทศ รวมทั้งการฝึกอบรมเพื่อเพิ่มพูนความรู้ทางด้านเทคนิคคอมพิวเตอร์มาโดยตลอดทำให้เนื้อหามีความสมบูรณ์ยิ่งขึ้น เพื่อให้ผู้ที่ปฏิบัติงานด้านความมั่นคงปลอดภัยของระบบสารสนเทศ และผู้ที่เกี่ยวข้องกับระบบสารสนเทศสามารถเข้าใจเกี่ยวกับการตรวจสอบระบบสารสนเทศและสามารถนำไปประยุกต์ใช้ในการปฏิบัติงานได้ดียิ่งขึ้น นอกจากนี้ยังมีเกมบทบาทการตรวจสอบระบบสารสนเทศเพื่อใช้เป็นกรณีศึกษาในการเรียนได้ ทั้งนี้ผู้ที่จะอ่านหนังสือเล่มนี้ควรมีพื้นฐานความรู้เกี่ยวกับคอมพิวเตอร์ และความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศมาก่อนแล้ว ส่วนความรู้เชิงลึกด้านเทคโนโลยีสารสนเทศนั้นเป็นองค์ความรู้ในสาขาวิชาอื่นจึงไม่ขอกล่าวในหนังสือเล่มนี้

ผู้เขียนหวังว่าหนังสือเล่มนี้จะเป็นแหล่งรวบรวมองค์ความรู้ด้านการตรวจสอบระบบสารสนเทศที่มีคุณค่าสำหรับทุกท่านต่อไป

นิตยา วงศ์ภินันท์วัฒนา

มกราคม 2561

wongpinn@tu.ac.th

บทนำ

ปัจจุบันมีการนำระบบสารสนเทศมาใช้ในองค์กรอย่างแพร่หลาย เพื่อเพิ่มประสิทธิภาพและประสิทธิผลของการดำเนินงานให้เจริญก้าวหน้า โดยระบบสารสนเทศเป็นระบบที่ทำหน้าที่จัดเก็บข้อมูล ประมวลผล และนำเสนอผลลัพธ์เพื่อให้ผู้บริหารระดับสูงใช้ในการตัดสินใจ องค์ประกอบของระบบสารสนเทศ ประกอบด้วย บุคลากร กระบวนการ ข้อมูล ซอฟต์แวร์ ฮาร์ดแวร์และองค์ประกอบระบบเครือข่ายคอมพิวเตอร์ ดังนั้นการที่ระบบสารสนเทศขององค์กรจะมีประสิทธิภาพหรือไม่จึงขึ้นอยู่กับองค์ประกอบของระบบสารสนเทศด้วย องค์กรจึงควรมีการควบคุม และตรวจสอบระบบสารสนเทศ เพื่อให้มั่นใจว่ามีการป้องกันความเสี่ยงที่อาจเกิดขึ้นได้ โดยการตรวจสอบระบบสารสนเทศ คือ กระบวนการเก็บรวบรวมหลักฐานสำหรับสิ่งผิดปกติที่เกิดขึ้นกับทรัพย์สินสารสนเทศ ซึ่งเทคนิคในการรวบรวมหลักฐานอาจทำโดย การสอบถาม การสอบทาน และการสังเกตการณ์ สำหรับวัตถุประสงค์ของการตรวจสอบระบบสารสนเทศเพื่อให้มั่นใจว่าองค์กรมี (1) การรักษาความลับของข้อมูล (2) ความถูกต้องครบถ้วนของข้อมูล (3) การทำให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้งาน (4) การดูแลรักษาทรัพย์สินสารสนเทศให้ปลอดภัย (5) การมีประสิทธิภาพและประสิทธิผลของระบบสารสนเทศ (6) ความเป็นส่วนตัวของข้อมูลของลูกค้า และ (7) การปฏิบัติตามกฎหมายและกฎข้อบังคับต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศ (Kanhere, 2009) ดังนั้นการตรวจสอบระบบสารสนเทศจึงเป็นส่วนหนึ่งของการตรวจสอบของผู้ตรวจสอบภายในและเป็นส่วนหนึ่งของการตรวจสอบรายงานทางการเงินของผู้สอบบัญชีรับอนุญาต (Singleton, 2009) กล่าวคือ ผู้สอบบัญชีรับอนุญาตจะเน้นการตรวจสอบเพื่อพิจารณาว่าสามารถเชื่อถือในความถูกต้องครบถ้วนของตัวเลขในรายงานทางการเงินที่จัดทำจากระบบสารสนเทศได้ ส่วนผู้ตรวจสอบภายในขององค์กร นอกจากความมั่นใจในความถูกต้องครบถ้วนของตัวเลขในรายงานทางการเงินแล้ว ยังเน้นการตรวจสอบเพื่อพิจารณาว่าระบบสารสนเทศปฏิบัติงานอย่างมีประสิทธิภาพและประสิทธิผลหรือไม่ รวมถึงการปฏิบัติตามกฎหมายและกฎข้อบังคับต่างๆ ขององค์กรและหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานภาครัฐ เป็นต้น โดยทั่วไปมักจะเรียกผู้ที่ทำหน้าที่ตรวจสอบระบบสารสนเทศว่า ผู้ตรวจสอบระบบสารสนเทศ (information systems auditor หรือ IS auditor) หรือผู้ตรวจสอบเทคโนโลยีสารสนเทศ (information technology auditor หรือ IT auditor) ดังนั้นการกล่าวถึงผู้ตรวจสอบในหนังสือนี้โดยไม่ได้เจาะจงว่าเป็นผู้ตรวจสอบภายในหรือผู้สอบบัญชีรับอนุญาต ให้หมายถึงผู้ตรวจสอบระบบสารสนเทศ นอกจากนี้ผู้ตรวจสอบยังสามารถปฏิบัติงานในฐานะเจ้าหน้าที่ความมั่นคงปลอดภัยระบบสารสนเทศ ซึ่งมีหน้าที่กำหนดการควบคุมและตรวจสอบระบบสารสนเทศด้วยตนเองในเบื้องต้น (Boccasam, 2003)

บทนำ

ผู้บริหารระบบสารสนเทศ เป็นผู้ที่ทำหน้าที่ควบคุมดูแลการบริหารงานด้านระบบสารสนเทศขององค์กร และให้คำแนะนำเกี่ยวกับกลยุทธ์ด้านระบบสารสนเทศแก่ประธานเจ้าหน้าที่บริหาร (chief executive officer หรือ CEO) โดยทั่วไปการเรียกชื่อตำแหน่งของผู้บริหารระบบสารสนเทศจะแตกต่างกันไปตามโครงสร้างและขนาดขององค์กร เช่น องค์กรขนาดใหญ่บางแห่งอาจเรียกว่า ประธานฝ่ายสารสนเทศ (chief information officer หรือ CIO) หรือเรียกว่ารองประธานเจ้าหน้าที่บริหารระบบสารสนเทศก็ได้ สำหรับองค์กรขนาดกลางและขนาดเล็กบางแห่งอาจมีการใช้ชื่อตำแหน่งว่า ผู้จัดการศูนย์คอมพิวเตอร์ หรือผู้บริหารศูนย์คอมพิวเตอร์ เป็นต้น ดังนั้นหนังสือเล่มนี้จึงกล่าวถึง ผู้ที่ทำหน้าที่ควบคุมดูแลการบริหารงานด้านระบบสารสนเทศ โดยไม่ระบุตำแหน่งว่า ผู้บริหารระบบสารสนเทศ ทั้งนี้การดำเนินงานของผู้บริหารระบบสารสนเทศจะมีผลต่อการดำเนินงานขององค์กรด้วย ซึ่งหากระบบสารสนเทศขององค์กรมีความถูกต้อง ครบถ้วนอย่างสมบูรณ์ โดยมีการรักษาความมั่นคงปลอดภัยที่ดีแล้ว จะทำให้ผู้บริหารระดับสูงมีข้อมูลที่ใช้ในการตัดสินใจดำเนินธุรกิจได้อย่างถูกต้อง และสามารถสร้างความได้เปรียบเหนือคู่แข่งขันได้ ดังนั้นการตรวจสอบการดำเนินงานของผู้บริหารระบบสารสนเทศจะทำให้ผู้ตรวจสอบมั่นใจได้ว่า องค์กรที่ตรวจสอบมีการรักษาความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศด้านต่างๆ อย่างเหมาะสมหรือไม่ ในการตรวจสอบการดำเนินงานของผู้บริหารระบบสารสนเทศนั้น ผู้ตรวจสอบจะตรวจสอบความเหมาะสมของการปฏิบัติหน้าที่ของผู้บริหารระบบสารสนเทศด้าน การวางแผน (planning) การจัดองค์กร (organizing) การเป็นผู้นำ (leading) และการควบคุม (controlling) ในบทนี้จะกล่าวถึง ความเสี่ยงและการควบคุมเกี่ยวกับการดำเนินงานของผู้บริหารระบบสารสนเทศ รวมทั้งแนวทางการตรวจสอบการดำเนินงานของผู้บริหารระบบสารสนเทศ

ความเสี่ยงและการควบคุมการดำเนินงานของผู้บริหารระบบสารสนเทศ

ความเสี่ยงและการควบคุมการดำเนินงานของผู้บริหารระบบสารสนเทศซึ่งสรุปจากหนังสือ *ความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศ* โดย นิตยา วงศ์ภินันท์วัฒนา (2563) มีดังนี้

บทนำ

องค์กรขนาดใหญ่มักจะนำระบบสารสนเทศมาใช้ในการดำเนินงานโดยติดตั้งคอมพิวเตอร์ขนาดใหญ่และอุปกรณ์ประกอบไว้ในห้องที่จัดทำขึ้นโดยเฉพาะในห้องคอมพิวเตอร์ พร้อมทั้งมีการปรับสภาพแวดล้อมภายในห้องซึ่งประกอบด้วย การมีระบบควบคุมการเข้าออกทางกายภาพ การติดตั้งระบบไฟฟ้าสำรอง เครื่องทำความเย็น สัญญาณเตือนภัย และเครื่องมือดับเพลิง โดยห้องดังกล่าวยังตั้งอยู่ภายในศูนย์คอมพิวเตอร์ ซึ่งมีเจ้าหน้าที่ปฏิบัติงานตามหน้าที่งานด้านต่างๆ เกี่ยวกับระบบสารสนเทศ ได้แก่ การจัดหาโปรแกรมประยุกต์ การปฏิบัติการคอมพิวเตอร์ การปฏิบัติการเครือข่าย การจัดเตรียมและป้อนข้อมูล การควบคุมงานบริการระบบสารสนเทศ และการเก็บรักษา ซึ่งหน้าที่งานเหล่านี้จัดได้ว่าเป็นงานด้านการปฏิบัติการระบบสารสนเทศที่อาจมีความเสี่ยงให้เกิดภัยต่อระบบสารสนเทศได้ ดังนั้นผู้ตรวจสอบจึงควรสอบทานว่าองค์ประกอบต่างๆ ในห้องคอมพิวเตอร์ทำหน้าที่อย่างมีประสิทธิภาพและประสิทธิผลหรือไม่ ในบทนี้จะกล่าวถึงความเสี่ยงและการควบคุมเกี่ยวกับการปฏิบัติการระบบสารสนเทศ รวมทั้งแนวทางการตรวจสอบด้านการปฏิบัติการระบบสารสนเทศ ซึ่งเป็นการตรวจสอบการควบคุมทั่วไป

ความเสี่ยงและการควบคุมด้านการปฏิบัติการระบบสารสนเทศ

ความเสี่ยงและการควบคุมด้านการปฏิบัติการระบบสารสนเทศซึ่งสรุปจากหนังสือ *ความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศ* โดย นิตยา วงศ์ภินันท์วัฒนา (2563) มีดังนี้

ตารางที่ 4.1 สรุปภัยคุกคามและการควบคุมการปฏิบัติการระบบสารสนเทศ

ความเสี่ยง	การควบคุม
การได้มาซึ่งโปรแกรมประยุกต์:	
ความเสี่ยงจากการโจมตีจุดอ่อนของการได้มาซึ่งโปรแกรมประยุกต์ไม่เหมาะสม ได้แก่ ความไม่เหมาะสมของการประเมินความเป็นไปได้ของโครงการ การออกแบบการประมวลผลโปรแกรมประยุกต์ การทดสอบโปรแกรมประยุกต์ และการแปลงระบบ จะก่อให้เกิดปัญหาข้อมูลไม่ถูกต้องครบถ้วน (Integrity) ข้อมูลไม่เป็นความลับ (confidentiality) ไม่มีข้อมูลให้งานใช้ได้เมื่อผู้มีสิทธิต้องการใช้ข้อมูล (availability)	- ควบคุมดูแลการได้มาซึ่งโปรแกรมประยุกต์ให้เหมาะสมตั้งแต่การประเมินความเป็นไปได้ของโครงการ การทดสอบโปรแกรมประยุกต์ และการควบคุมการแปลงระบบ

บทนำ

ปัจจุบันมีการนำระบบเครือข่ายคอมพิวเตอร์หรือเรียกกันสั้นๆ ว่า “ระบบเครือข่าย” มาใช้กันอย่างแพร่หลายทำให้ผู้ใช้งานสามารถใช้ข้อมูลและทรัพยากรในระบบเครือข่ายคอมพิวเตอร์ร่วมกันได้อย่างรวดเร็ว เช่น ใช้เครื่องพิมพ์หรือโปรแกรมประยุกต์ เป็นต้น แต่การเชื่อมโยงอุปกรณ์ทางคอมพิวเตอร์เข้าด้วยกันอาจมีความเสี่ยงใหม่ๆ เกิดขึ้นซึ่งจะส่งผลต่อความถูกต้องครบถ้วน การเก็บรักษาความลับของข้อมูล และการมีระบบเครือข่ายคอมพิวเตอร์ที่พร้อมให้ใช้งานได้ ดังนั้นผู้ตรวจสอบจึงควรให้ความสนใจในการตรวจสอบระบบเครือข่ายคอมพิวเตอร์ด้วย ระบบเครือข่ายคอมพิวเตอร์ที่นิยมใช้กันมาก คือ (1) ระบบเครือข่ายเฉพาะที่ (local area network หรือ LAN) เป็นระบบเครือข่ายที่ใช้ภายในพื้นที่เดียวกันหรือใกล้เคียงกัน โดยเชื่อมโยงอุปกรณ์เข้าด้วยกันทั้งในรูปแบบระบบเครือข่ายมีสาย (wired local area network หรือ wired LAN) และระบบเครือข่ายไร้สายหรือแลนไร้สาย (wireless local area network หรือ WLAN) ก็ได้ (2) ระบบเครือข่ายบริเวณกว้างหรือระยะไกล (wide area network หรือ WAN) เป็นระบบเครือข่ายที่ครอบคลุมพื้นที่บริเวณกว้างในระยะไกลได้ทั่วโลกโดยเชื่อมโยงอุปกรณ์ระหว่างกันในรูปแบบระบบเครือข่ายไร้สาย ในบทนี้จะกล่าวถึงความเสี่ยงและการควบคุมเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์ทั้งแบบมีสายและแบบไร้สาย รวมทั้งแนวทางการตรวจสอบระบบเครือข่ายคอมพิวเตอร์

ความเสี่ยงและการควบคุมระบบเครือข่ายคอมพิวเตอร์

ความเสี่ยงและการควบคุมระบบเครือข่ายคอมพิวเตอร์ซึ่งสรุปจากหนังสือ *ความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศ* โดย นิตยา วงศ์ภินันท์วัฒนา (2563) มีดังนี้

บทนำ

การที่คอมพิวเตอร์และอุปกรณ์ต่างๆ จะเชื่อมต่อเป็นระบบเครือข่ายคอมพิวเตอร์เพื่อให้สามารถปฏิบัติงานได้นั้น จำเป็นต้องมีระบบปฏิบัติการเพื่อทำหน้าที่ในการบริหารจัดการการใช้งานทรัพยากรต่างๆ ในระบบเครือข่ายรวมทั้งบริการอินเทอร์เน็ต ดังนั้นระบบปฏิบัติการจึงมีความสำคัญอย่างมาก เนื่องจากเป็นด่านหน้าในการติดต่อสื่อสารระหว่างคอมพิวเตอร์และอุปกรณ์ต่างๆ ในระบบเครือข่ายคอมพิวเตอร์ และมักเป็นช่องทางที่จะเกิดความเสี่ยงในลำดับต้นๆ ระบบปฏิบัติการจะมีหน้าที่งานที่ต้องกำหนดค่าการทำงานของตัวแปร (configuration) เพื่อให้สามารถปฏิบัติงานได้และมีการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม ดังนั้นผู้ตรวจสอบจึงควรตรวจสอบระบบปฏิบัติการด้วยเช่นกัน ปัจจุบันมีการนำระบบปฏิบัติการคอมพิวเตอร์และระบบปฏิบัติการเครือข่ายมารวมกันเป็นระบบปฏิบัติการเดียว และเรียกว่าระบบปฏิบัติการ ดังนั้นเมื่อกล่าวถึงคำว่า “ระบบปฏิบัติการ” ในหนังสือเล่มนี้จึงหมายถึงระบบปฏิบัติการเครือข่ายด้วย ในบทนี้จะกล่าวถึง ความเสี่ยงและการควบคุมที่เกี่ยวกับระบบปฏิบัติการ รวมทั้งแนวทางการตรวจสอบระบบปฏิบัติการ

ความเสี่ยงและการควบคุมระบบปฏิบัติการ

ความเสี่ยงและการควบคุมระบบปฏิบัติการซึ่งสรุปจากหนังสือ *ความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศ* โดย นิตยา วงศ์ภินันท์วัฒนา (2563) มีดังนี้

บทนำ

ฐานข้อมูลเป็นองค์ประกอบหนึ่งของระบบสารสนเทศที่มีความสำคัญเนื่องจากฐานข้อมูลเป็นการรวบรวมกลุ่มข้อมูลที่มีความสัมพันธ์กันไว้ด้วยกันในรูปของตารางหลายๆ ตาราง แทนการเก็บข้อมูลที่ซ้ำซ้อนกันของแฟ้มข้อมูล ทำให้การจัดการและปรับปรุงฐานข้อมูลทำได้ง่าย รวมทั้งสามารถใช้ข้อมูลในฐานข้อมูลร่วมกันได้สะดวกขึ้น โดยมีผู้บริหารฐานข้อมูลเป็นผู้ควบคุมดูแลการบริหารงานของฐานข้อมูลทั้งหมด ทั้งนี้การเรียกชื่อตำแหน่งผู้บริหารฐานข้อมูลของแต่ละองค์กรจะมีความแตกต่างกันตามโครงสร้างและขนาดขององค์กรซึ่งบางองค์กรอาจเรียกผู้ที่ทำหน้าที่นี้ว่าหัวหน้าเจ้าหน้าที่จัดการฐานข้อมูลก็ได้ สำหรับการรักษาความมั่นคงปลอดภัยของฐานข้อมูลจำเป็นจะต้องทราบถึงการควบคุมที่เหมาะสมก่อนแม้ว่าฐานข้อมูลจะได้รับการปกป้องเมื่อองค์กรมีการบริหารด้านระบบสารสนเทศอย่างเหมาะสมแล้วก็ตามแต่ฐานข้อมูลก็มีโอกาสที่จะได้รับความเสี่ยงเช่นกัน ดังนั้นผู้ตรวจสอบควรตรวจสอบว่าฐานข้อมูลมีช่องโหว่ที่ใดที่ต้องป้องกันข้อมูลที่อยู่ภายในฐานข้อมูลให้มีความปลอดภัยในบทนี้จะกล่าวถึงความเสี่ยงและการควบคุมที่เกี่ยวกับฐานข้อมูลรวมทั้งแนวทางการตรวจสอบฐานข้อมูล

ความเสี่ยงและการควบคุมฐานข้อมูล

ความเสี่ยงและการควบคุมฐานข้อมูลซึ่งสรุปจากหนังสือ *ความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศ* โดย นิตยา วงศ์ภินันท์วัฒนา (2563) มีดังนี้

บทนำ

โปรแกรมประยุกต์ คือ ระบบที่ธุรกิจนำมาใช้เพื่อสนับสนุนกิจกรรมทางธุรกิจ เช่น การซื้อและขายสินค้า การรับและจ่ายชำระเงิน การผลิต และการควบคุมสินค้าคงเหลือ เป็นต้น ทั้งนี้ธุรกิจอาจได้โปรแกรมประยุกต์มาจากการซื้อโปรแกรมสำเร็จรูปหรือจัดสร้างโปรแกรมประยุกต์ขึ้นมาเอง นอกจากนี้โปรแกรมประยุกต์อาจมีความซับซ้อนมากหรือน้อยขึ้นอยู่กับการนำมาใช้ให้เหมาะสมกับขนาดของธุรกิจ เนื่องจากการพัฒนาโปรแกรมประยุกต์เป็นการพัฒนาด้วยภาษาโปรแกรม (programming language) แพลตฟอร์ม (platform) และฐานข้อมูลที่แตกต่างกัน ดังนั้นโปรแกรมประยุกต์เหล่านี้จะต้องมีการควบคุมที่แตกต่างกันออกไป ผู้ตรวจสอบจึงมีหน้าที่สอบทานว่าโปรแกรมประยุกต์ต่างๆ ประมวลผลข้อมูลครบถ้วนและถูกต้องหรือไม่ ในบทนี้จะกล่าวถึง ความเสี่ยงและการควบคุมโปรแกรมประยุกต์ รวมทั้งแนวทางการตรวจสอบโปรแกรมประยุกต์

ความเสี่ยงและการควบคุมโปรแกรมประยุกต์

ความเสี่ยงและการควบคุมโปรแกรมประยุกต์ซึ่งสรุปจากหนังสือ *ความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศ* โดย นิตยา วงศ์ภานันท์วัฒนา (2563) มีดังนี้

ตารางที่ 8.1 สรุปภัยคุกคามและการควบคุมโปรแกรมประยุกต์

ความเสี่ยง	การควบคุม
ความเสี่ยงและการควบคุมโปรแกรมประยุกต์ขั้นต้น:	
ความเสี่ยงจากการโจมตีจุดอ่อนของการที่ข้อมูลนำเข้าไม่ได้รับการอนุมัติหรือไม่มีการควบคุมความถูกต้องครบถ้วน ก่อให้เกิดปัญหาข้อมูลไม่ถูกต้องครบถ้วน (integrity)	การควบคุมแบบฟอร์มที่ใช้ในการกรอกข้อมูลก่อนการบันทึกข้อมูลเข้าสู่ระบบคอมพิวเตอร์ มีดังนี้ - การออกแบบแบบฟอร์ม - การยกเลิกและจัดเก็บเอกสาร - การอนุมัติและการควบคุมการแบ่งแยกหน้าที่ - การสอบทานด้วยสายตา

การตรวจสอบระบบสารสนเทศ

หนังสือ*การตรวจสอบระบบสารสนเทศ*เล่มนี้ มีเนื้อหาครอบคลุมการตรวจสอบระบบสารสนเทศที่องค์กรต่างๆ นำมาใช้งานในปัจจุบัน โดยเนื้อหาของหนังสือจะเน้นในเรื่องการดำเนินการตรวจสอบระบบสารสนเทศ เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบ การตรวจสอบการดำเนินงานของผู้บริหารด้านระบบสารสนเทศ การตรวจสอบการปฏิบัติการระบบสารสนเทศ การตรวจสอบระบบเครือข่ายคอมพิวเตอร์ การตรวจสอบระบบปฏิบัติการเครือข่าย การตรวจสอบฐานข้อมูล การตรวจสอบโปรแกรมประยุกต์ และรายงานการตรวจสอบระบบสารสนเทศ หนังสือนี้ได้อธิบายความรู้ทางการตรวจสอบระบบสารสนเทศในระดับที่เหมาะสมกับนักศึกษาสาขาวิชาการบัญชีและบริหารธุรกิจ และผู้ที่เกี่ยวข้องกับการบริหารระบบสารสนเทศ ซึ่งมีพื้นฐานความรู้เกี่ยวกับคอมพิวเตอร์และความมั่นคงปลอดภัยและการควบคุมระบบสารสนเทศในระดับหนึ่งมาก่อนแล้ว

ดร.นิตยา วงศ์ภินันท์พิมนา

ศาสตราจารย์ประจำภาควิชาระบบสารสนเทศเพื่อการจัดการ
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

การศึกษา

PhD in Information Systems จาก The University of Queensland, Australia
MCom in Business Information Systems จาก University of Wollongong, Australia
บัญชีมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์
บัญชีบัณฑิต (เกียรตินิยมอันดับหนึ่ง) มหาวิทยาลัยธรรมศาสตร์

ประสบการณ์

ผู้ตรวจสอบผู้ช่วย, สำนักงานสอบบัญชี SGVN ณ ถลาง
ผู้ตรวจการธนาคารพาณิชย์, ส่วนตรวจสอบธนาคารพาณิชย์, ธนาคารแห่งประเทศไทย
นักวิเคราะห์ระบบ, Esso Standard Thailand Co., Ltd.
(An Affiliate of Exxon Corporation)

ISBN 978-616-602-138-7
9 786166 021387
ราคา 300 บาท
หมวดพาณิชยศาสตร์

http://www.thammasatpress.tu.ac.th