

	หน้า
คำนำ	iii
บทที่ 1 ภาพในแนวกว้างของการควบคุมระบบสารสนเทศ	1
1. วัตถุประสงค์ของบท	1
2. บทนำ	1
3. ความจำเป็นสำหรับการควบคุมและการตรวจสอบระบบสารสนเทศ	2
4. บุคคลที่ก่อให้เกิดภัยคุกคาม	7
5. สาเหตุของการโจมตีระบบสารสนเทศ	9
6. วัตถุประสงค์หลักของการควบคุมระบบสารสนเทศ	11
7. แนวคิดหรือลักษณะของการควบคุม	13
8. การรักษาความปลอดภัย	15
9. ผลของการใช้ระบบสารสนเทศต่อการควบคุมภายใน	17
10. การควบคุมเฉพาะของระบบสารสนเทศ	20
11. มาตรฐาน แนวทางปฏิบัติและกรอบวิธีปฏิบัติ	27
ภาคผนวกที่ 1 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	31
ภาคผนวกที่ 2 บริการ วินโดวส์เอ็กพีและข้อเสนอแนะในการกำหนดบริการ	34
ภาคผนวกที่ 3 กรอบวิธีปฏิบัติของ COSO, CobiT และมาตรฐานการตรวจสอบด้านระบบสารสนเทศ	35
บทที่ 2 ภัยคุกคามต่อระบบสารสนเทศ	63
1. วัตถุประสงค์ของบท	63
2. บทนำ	63
3. ความรู้เบื้องต้นเกี่ยวกับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ	63
4. ภัยคุกคามต่อระบบสารสนเทศ	68
บทที่ 3 การดำเนินการตรวจสอบระบบสารสนเทศ	93
1. วัตถุประสงค์ของบท	93
2. บทนำ	93
3. ความหมายของการตรวจสอบระบบสารสนเทศ	94
4. ภาพในแนวกว้างของขั้นตอนการตรวจสอบ	95
5. ผลของคอมพิวเตอร์ต่อการตรวจสอบ	101
6. รากฐานของการตรวจสอบระบบสารสนเทศ	102
7. การจัดการกับความซับซ้อน	105
8. การประเมินความเสี่ยงทางระบบสารสนเทศ	110

9. เครื่องมือในการหาหลักฐาน	133
ภาคผนวกที่ 1 การเปรียบเทียบความแตกต่างระหว่างการตรวจสอบแบบเดิม และแบบประเมินความเสี่ยง	135
ภาคผนวกที่ 2 การประเมินความเสี่ยงตามแบบของ ISACA ในลักษณะของ การให้คะแนนความเสี่ยง	136
ภาคผนวกที่ 3 การประเมินความเสี่ยงตามแบบ CobIT	153
ภาคผนวกที่ 4 การประเมินความเสี่ยงตามแบบ OCTAVE	158
บทที่ 4 การควบคุมและตรวจสอบการดำเนินงานของผู้บริหาร	161
1. วัตถุประสงค์ของบท	161
2. คำนำ	161
3. หน้าที่งานของผู้บริหารด้านระบบสารสนเทศ	161
4. ความเสี่ยงของการดำเนินงานของผู้บริหาร	178
5. การตรวจสอบการดำเนินงานของผู้บริหาร	179
ภาคผนวกที่ 1 หลักการและรูปแบบสำหรับจัดตั้งหน้าที่งานทางระบบสารสนเทศ	182
ภาคผนวกที่ 2 นโยบายการรักษาความปลอดภัยและวิธีการปฏิบัติ	185
ภาคผนวกที่ 3 การคิดค่าใช้จ่ายที่เหมาะสมกับสภาพขององค์กร	204
บทที่ 5 การควบคุมและตรวจสอบการปฏิบัติการระบบสารสนเทศ	209
1. วัตถุประสงค์ของบท	209
2. คำนำ	209
3. การจัดการด้านโปรแกรมประยุกต์	209
4. การจัดการด้านการรักษาความปลอดภัย	229
5. การจัดการด้านปฏิบัติการ	242
ภาคผนวกที่ 1 การเลือกชุดซอฟต์แวร์สำเร็จรูป	255
ภาคผนวกที่ 2 ความเสี่ยงและการควบคุม OO	258
ภาคผนวกที่ 3 การทำให้ระบบกลับสู่สภาพเดิมจากภัยพิบัติ	264
บทที่ 6 การควบคุมและตรวจสอบระบบเครือข่ายคอมพิวเตอร์	271
1. วัตถุประสงค์ของการศึกษา	271
2. คำนำ	271
3. การควบคุมระบบเครือข่ายคอมพิวเตอร์	272
4. การควบคุมโครงสร้างของเครือข่าย	293
5. การตรวจสอบด้านการสื่อสารข้อมูล	308
ภาคผนวก บริการใบรับรองอิเล็กทรอนิกส์ของบริษัท กสท โทรคมนาคม จำกัด (มหาชน)	312

บทที่ 7 การควบคุมและตรวจสอบระบบปฏิบัติการเครือข่าย	313
1. วัตถุประสงค์ของการศึกษา	313
2. คำนำ	313
3. หน้าที่หลักของระบบปฏิบัติการเครือข่าย	314
4. การควบคุมความปลอดภัยระบบปฏิบัติการเครือข่าย	317
5. ความเสี่ยงและการควบคุมการใช้บริการอินเทอร์เน็ต	323
6. การรักษาความปลอดภัยของแลนไร้สาย	330
7. การตรวจสอบระบบปฏิบัติการเครือข่ายเบื้องต้น	333
บทที่ 8 การควบคุมและตรวจสอบฐานข้อมูล	349
1. วัตถุประสงค์ของการศึกษา	349
2. บทนำ	349
3. ลักษณะทั่วไปของฐานข้อมูล	349
4. ความเสี่ยงที่อาจเกิดกับฐานข้อมูล	356
5. การควบคุมฐานข้อมูล	361
6. การตรวจสอบฐานข้อมูล	389
7. การควบคุมและตรวจสอบคลังข้อมูล	391
บทที่ 9 การควบคุมและตรวจสอบโปรแกรมประยุกต์	399
1. วัตถุประสงค์ของการศึกษา	399
2. คำนำ	399
3. ความเสี่ยงของระบบโปรแกรมประยุกต์	401
4. การควบคุมข้อมูลนำเข้า	402
5. การควบคุมการประมวลผล	420
6. การควบคุมผลลัพธ์	426
7. การตรวจสอบโปรแกรมประยุกต์	435
ภาคผนวก การควบคุมและตรวจสอบการรักษาความปลอดภัยการเข้าถึงทางตรรกะของโปรแกรม SAP R/3	437
บทที่ 10 การนำเทคโนโลยีมาใช้ในการตรวจสอบ	439
1. วัตถุประสงค์ของการศึกษา	439
2. บทนำ	439
3. โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป	440
4. โปรแกรมตรวจสอบเฉพาะเรื่อง	442
5. โปรแกรมอรรถประโยชน์	443
6. ข้อมูลทดสอบ	447
7. เทคนิคการใช้คอมพิวเตอร์ช่วยในการตรวจสอบระหว่างการเกิดรายการ	448

8. การตรวจสอบโปรแกรม.....	452
9. เทคนิคการทำเหมืองข้อมูลเพื่อการตรวจสอบ.....	455
10. เทคนิคการทดสอบทะลุทะลวง.....	456
11. โปรแกรมด้านอื่น ๆ เพื่อการตรวจสอบ.....	469
ภาคผนวกที่ 1 การใช้งานโปรแกรม ACL Version 7.....	473
ภาคผนวกที่ 2 วิธีการและเครื่องมือสำหรับการทดสอบทะลุทะลวง.....	480
บทที่ 11 จรรยาบรรณที่เกี่ยวกับการรักษาความปลอดภัยทางด้านคอมพิวเตอร์.....	499
1. วัตถุประสงค์ของการศึกษา.....	499
2. ความหมายของจรรยาบรรณ.....	499
3. การตัดสินใจที่เกี่ยวกับจรรยาบรรณ.....	502
4. หลักการที่นำไปใช้ในการพิจารณาจรรยาบรรณ.....	502
5. ตัวอย่างของการพิจารณาจรรยาบรรณ.....	503
6. องค์การที่เกี่ยวข้องกับจรรยาบรรณ.....	505
7. บัญญัติ 10 ประการของจรรยาบรรณทางคอมพิวเตอร์.....	507
บรรณานุกรม.....	509