



กิจกรรมประจำชุดวิชา 96404

การตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน

ภาคปลาย ปีการศึกษา 2564

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

## คำนำ

เนื่องด้วยมหาวิทยาลัยสุโขทัยธรรมมาธิราช มุ่งให้ผู้เรียนและนักศึกษาได้มีส่วนร่วมในกระบวนการศึกษาเล่าเรียนแบบครบวงจร ตั้งแต่ก่อนเรียน ระหว่างเรียน และหลังจากเรียนเสร็จสิ้นไปแล้ว โดยจัดระบบการประเมินครบทั้ง 3 ส่วน ได้แก่ การประเมินก่อนเรียน การประเมินระหว่างเรียน และประเมินหลังเรียน

การประเมินกิจกรรม เป็นส่วนหนึ่งของการวัดผลสัมฤทธิ์ทางการเรียนสุดท้าย จึงกำหนดให้นักศึกษาทำกิจกรรมภาคปฏิบัติตามที่กำหนดให้ โดยมีวัตถุประสงค์เพื่อให้นักศึกษามีความสามารถ ดังนี้

1. สร้างหรือประมวลเนื้อหาสาระของเอกสารการสอนทั้งชุดวิชาหรือกลุ่มเนื้อหาในกลุ่มใดกลุ่มหนึ่ง
2. ประยุกต์ความรู้จากเอกสารการสอนเพื่อจัดทำโครงการพัฒนางานอย่างใดอย่างหนึ่งที่นักศึกษาทำ
3. พัฒนาระบบ โครงการ ชิ้นงาน ฯลฯ ตามกระบวนการหรือขั้นตอนที่แสดงไว้ในหน่วยใดหน่วยหนึ่งของเอกสารการสอน
4. คิด วิเคราะห์ นำเสนอข้อมูลและความคิดในเชิงสร้างสรรค์

นอกจากนี้การทำกิจกรรมประจำชุดวิชายังทำให้นักศึกษาได้ศึกษาเอกสารการสอนตั้งแต่ต้นภาคการศึกษา และจากการวิจัยพบว่านักศึกษาที่ทำกิจกรรมจะมีโอกาสสอบผ่านในปลายภาคมากกว่านักศึกษาที่ไม่ทำกิจกรรม

คณะกรรมการบริหารชุดวิชา การตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน ขอให้นักศึกษาทุกท่านประสบความสำเร็จในการศึกษาชุดวิชานี้ และสามารถนำความรู้ไปเป็นประโยชน์ต่อการดำเนินชีวิตและการประกอบอาชีพสืบไป

คณะกรรมการบริหารชุดวิชา

การตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน

11 มกราคม 2565

## 1. การประเมินผล

เกณฑ์การให้คะแนนกิจกรรมจะพิจารณาจากการตอบที่ตรงประเด็นคำถาม การครอบคลุมความถูกต้องของคำตอบ ความชัดเจนของการนำเสนอ ความละเอียดประณีตของชิ้นงาน

**นักศึกษาที่เลือกแผนการสอน ก2 และ ก3 ไม่ต้องทำกิจกรรมประจำชั้วติวิชา** และมหาวิทยาลัยไม่บังคับให้นักศึกษาทุกคนต้องทำกิจกรรม นักศึกษาอาจเลือกทำหรือไม่ทำก็ได้ โดยการประเมินผลปลายภาคสำหรับชั้วติวิชานี้ แบ่งออกเป็น 2 กรณี

**กรณีที่ 1 นักศึกษาทำกิจกรรม** มหาวิทยาลัยจะแบ่งคะแนนออกเป็น 2 ส่วน ส่วนแรกจากคะแนนสอบปลายภาค คิดร้อยละ 80 และส่วนที่ 2 จากคะแนนกิจกรรมร้อยละ 20 สำหรับคะแนนกิจกรรมจะนำไปใช้ทั้งการประเมินผลสอบไล่และสอบซ่อม นักศึกษาที่มีได้ส่งกิจกรรมในการสอบไล่จะส่งกิจกรรมเพื่อเป็นคะแนนในการสอบซ่อมไม่ได้

**กรณีที่ 2 นักศึกษาไม่ทำกิจกรรม** มหาวิทยาลัยจะประเมินผลจากการสอบปลายภาคเพียงอย่างเดียว

ในการประเมินผลสอบปลายภาค นักศึกษาทั้งกลุ่มที่ทำกิจกรรมและไม่ทำกิจกรรม จะได้รับการประเมินผลโดยใช้ข้อสอบฉบับเดียวกัน นักศึกษากลุ่มที่ทำกิจกรรมมีคะแนนเต็ม 80 คะแนน ส่วนนักศึกษากลุ่มที่ไม่ทำกิจกรรมมีคะแนนเต็ม 100 คะแนน

สำหรับนักศึกษาที่ทำกิจกรรมมหาวิทยาลัยจะพิจารณาให้นักศึกษาได้ประโยชน์สูงสุด โดยการนำคะแนนสอบปลายภาคของนักศึกษาเพียงอย่างเดียวมาเปรียบเทียบกับความคิดคะแนนสอบปลายภาครวมกับคะแนนกิจกรรม แล้วนำคะแนนส่วนที่มากกว่าไปใช้ในการตัดสินผลการสอบให้กับนักศึกษา ดังตัวอย่างต่อไปนี้

**ตัวอย่างที่ 1** นักศึกษาได้คะแนนกิจกรรม 18 คะแนน และทำข้อสอบได้ 65 ข้อ (คิดเป็น  $\frac{65}{120} \times 80 = 43.33$  คะแนน) นักศึกษาจะได้คะแนนกิจกรรมรวมกับคะแนนสอบปลายภาค =  $18 + 43.33 = 61.33$  คะแนน นั่นคือ *สอบผ่าน*

กรณีที่นักศึกษาไม่ได้ทำกิจกรรมประจำชั้วติวิชา จะคิดคะแนนจากการสอบปลายภาคเพียงอย่างเดียว นักศึกษาทำข้อสอบได้ 65 ข้อ จะได้  $\frac{65}{120} \times 100 = 54.17$  คะแนน นั่นคือ *สอบไม่ผ่าน*

**ตัวอย่างที่ 2** นักศึกษาได้คะแนนกิจกรรม 9 คะแนน และทำข้อสอบได้ 75 ข้อ (คิดเป็น  $\frac{75}{120} \times 80 = 50.00$  คะแนน) นักศึกษาจะได้คะแนนกิจกรรมรวมกับคะแนนสอบปลายภาค =  $9 + 50.00 = 59.00$  คะแนน

กรณีคิดคะแนนจากการสอบปลายภาคเพียงอย่างเดียว นักศึกษาจะได้  $\frac{75}{120} \times 100 = 62.50$  คะแนน

มหาวิทยาลัยจะเลือกให้นักศึกษาได้คะแนน 62.50 คะแนน นั่นคือ *สอบผ่าน*

## 2. การส่งกิจกรรมประจำชุดวิชา

ให้นักศึกษาดำเนินการดังนี้

1. ให้นักศึกษาส่งกิจกรรมประจำชุดวิชาฉบับจริงไปยังมหาวิทยาลัยและสำเนากิจกรรมที่ทำเสร็จแล้ว เก็บไว้เป็นหลักฐาน 1 ชุด
2. การส่งกิจกรรมประจำชุดวิชาภายใน วันที่ 30 เมษายน 2565
3. ให้จัดทำหน้าปกรายงานให้มีข้อความตามตัวอย่างที่แนบมา
4. ส่งกิจกรรมที่ทำเสร็จเรียบร้อยแล้วด้วยตนเอง ณ สำนักบริการการศึกษา มหาวิทยาลัยสุโขทัยธรรมาธิราช หรือส่งทางไปรษณีย์ลงทะเบียน โดยเจ้าหน้าที่ของดังนี้

ศูนย์บริการการสอนทางไปรษณีย์  
สำนักบริการการศึกษา  
มหาวิทยาลัยสุโขทัยธรรมาธิราช  
ตำบลบางพูด อำเภอปากเกร็ด  
จังหวัดนนทบุรี 11120  
( กิจกรรมประจำชุดวิชา 96404 การตรวจสอบระบบงานคอมพิวเตอร์  
และการควบคุมภายใน  
สาขาวิชาวิทยาศาสตร์และเทคโนโลยี )

หรือส่งผ่านช่องทางออนไลน์ของเว็บไซต์ที่มหาวิทยาลัยกำหนดไว้

5. นักศึกษาสามารถตรวจสอบว่าสำนักบริการการศึกษาได้รับกิจกรรมที่นักศึกษาส่งไปแล้วหรือยัง โดยโทรศัพท์สอบถามที่หมายเลข 0-2982-9633 หรือโทรศัพท์ติดต่อสำนักบริการการศึกษา หมายเลข 0-2-504-7621 หรือโทรศัพท์ติดต่อศูนย์สารสนเทศ หมายเลข 0-2504-7788 หรือ e-mail: [ic.proffice@stou.ac.th](mailto:ic.proffice@stou.ac.th) หรือตรวจสอบผ่านระบบสารสนเทศได้ที่ <https://regis.stou.ac.th/STOU/login.jsp>

## ปกรายงาน

กิจกรรมประจำชุดวิชา 96404

การตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ภาคปลาย ปีการศึกษา 2564

ชื่อนักศึกษา.....

รหัสประจำตัวนักศึกษา

--	--	--	--	--	--	--	--	--	--	--

ที่อยู่ .....

.....

โทรศัพท์ (ถ้ามี) .....

ข้าพเจ้าขอยอมรับการตัดสินผลคะแนนการทำกิจกรรมประจำชุดวิชา

จากผู้ประเมินถือเป็นที่สุด

ลงชื่อ.....

(.....)

### 3. เนื้อหากิจกรรม

**คำชี้แจง** กิจกรรมมีทั้งหมด 10 กิจกรรม ให้นักศึกษาทำกิจกรรมทุกข้อ  
โดยเขียนคำตอบลงในเอกสารฉบับนี้เท่านั้น

#### กิจกรรมที่ 1 (ศึกษาเอกสารการสอนหน่วยที่ 1)

**จงจับคู่ให้ถูกต้อง** (โดยนำตัวเลือกด้านขวาไปเติมหน้าข้อด้านซ้ายที่มีความเกี่ยวข้องกัน)

- |   |   |
|---|---|
| _____ 1. ความหมายของ R ในแนวคิด IT GRC  | A. หลักนิติธรรม A                                     |
| _____ 2. ประเภทของการควบคุมจำแนกตามขอบเขตของงาน   | B. หลักเปิดเผย/โปร่งใส B                              |
| _____ 3. ประเภทของการควบคุมจำแนกตามวัตถุประสงค์ของการควบคุม   | C. หลักการกระจายอำนาจ C                               |
| _____ 4. การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ  | D. หลักการมีส่วนร่วม D                                |
| _____ 5. หลังจากเสร็จสิ้นการทดสอบแล้ว ต้องจัดทำรายงานผลการ<br>ตรวจสอบเพื่อส่งมอบให้กับผู้บริหารหรือผู้ว่าจ้าง         | E. ผู้สอบบัญชี K                                      |
| _____ 6. คุณลักษณะที่พึงประสงค์ของระบบราชการไทย 8 ประการ  | F. ผู้ตรวจสอบภายใน                                    |
| _____ 7. มาตรฐานด้านคุณสมบัติ มาตรฐานด้านการปฏิบัติงาน และ<br>มาตรฐานด้านการนำไปใช้                                   | G. มาตรฐานสากลของการปฏิบัติงาน<br>วิชาชีพตรวจสอบภายใน |
| _____ 8. บุคคลภายนอกหรือภายในองค์กร ที่ทำหน้าที่ตรวจสอบการ<br>ดำเนินงานต่างๆ ขององค์กร ว่าเป็นไปตามที่กำหนดไว้หรือไม่ | H. I AM READY   |
| _____ 9. มอบอำนาจในการตัดสินใจให้แก่ผู้ปฏิบัติงานในระดับต่างๆ<br>อย่างเหมาะสม   | I. Compliance   |
| _____ 10. การปฏิบัติงานตามอำนาจทางกฎหมาย กฎระเบียบ ข้อบังคับ<br>อย่างเคร่งครัด ด้วยความเป็นธรรมและไม่เลือกปฏิบัติ     | J. Governance   |
|   | K. Risk management                                    |
|   | L. ช่วงวางแผนการตรวจสอบ                               |
|   | M. ช่วงทดสอบการควบคุม O                               |
|   | N. ช่วงทดสอบเนื้อหาสาระและสรุปผล                      |
|   | O. เพื่อป้องกัน เพื่อค้นหา เพื่อแก้ไข                 |
|   | P. การควบคุมทั่วไป และการควบคุม<br>ระบบงานประยุกต์    |

## กิจกรรมที่ 2 (ศึกษาเอกสารการสอนหน่วยที่ 3 และ 4)

จงใส่เครื่องหมายถูก (✓) หน้าข้อที่ถูกต้อง และใส่เครื่องหมายผิด (X) หน้าข้อที่ผิด

- \_\_\_ 1. CobiT คือ กรอบการดำเนินงานด้านการใช้เทคโนโลยีสารสนเทศให้สอดคล้องกับวัตถุประสงค์ในการดำเนินงานขององค์กร
- \_\_\_ 2. COSO คือ กรอบการดำเนินงานด้านการควบคุมภายในและบริหารความเสี่ยงทั่วทั้งองค์กร
- \_\_\_ 3. ผู้จัดการข้อมูล มีหน้าที่รับผิดชอบประสิทธิผลของการใช้งานฐานข้อมูล ดูแลจัดการเรื่องการออกแบบ และการเข้าถึงระบบฐานข้อมูล ให้ความช่วยเหลือแก่ผู้ใช้งานในการใช้งานฐานข้อมูลได้อย่างดี
- \_\_\_ 4. ITIL คือ กรอบการดำเนินงานด้านการจัดการงานบริการเทคโนโลยีสารสนเทศ ที่เพิ่มประสิทธิภาพ เพิ่มความพึงพอใจแก่ผู้รับบริการ และประหยัดค่าใช้จ่าย
- \_\_\_ 5. การแยกการดำเนินงานระหว่างบอร์ดบริหารกับคณะกรรมการขับเคลื่อนด้านเทคโนโลยีสารสนเทศ ออกจากกัน คือ การแยกการกำกับดูแลกิจการออกจากการบริหารจัดการ
- \_\_\_ 6. โดเมน DSS ใน CobiT 5 ได้แก่ การส่งมอบ (Deliver) การให้บริการ (Service) และการสนับสนุน (Support)
- \_\_\_ 7. ข้อดีของการจัดโครงสร้างองค์กรส่วนงานเทคโนโลยีสารสนเทศแบบกระจายศูนย์ คือ ฝ่ายบริหารสามารถควบคุมการดำเนินงานได้สะดวก
- \_\_\_ 8. องค์กรที่มีรูปแบบการทำงานที่ต้องปรับตัวและเปลี่ยนแปลงมากอยู่ตลอดเวลา ระบบสารสนเทศที่ใช้งานปัจจุบันและที่จะนำมาใช้งานในอนาคตมีความสำคัญมาก จำนวนแผนงานระบบสารสนเทศมีน้อย และเน้นความจำเป็นในส่วนของทรัพยากรและระบบงานที่ต้องการใช้งานในระยะสั้น
- \_\_\_ 9. องค์กรที่มีรูปแบบการทำงานเชิงกลยุทธ์ ผู้บริหารระดับสูงค่อนข้างไม่สำคัญ ส่วนสมาชิกอาจเลือกจากการเป็นตัวแทนของฝ่ายบริหารระดับกลาง
- \_\_\_ 10. เมื่อบุคลากรในส่วนงานเทคโนโลยีสารสนเทศยื่นใบลาออก ถือเป็นการสิ้นสุดหน้าที่ในการปฏิบัติงาน โดยอัตโนมัติ ไม่จำเป็นต้องยกเลิกสิทธิ์ในการเข้าถึงข้อมูลหรือระบบสารสนเทศ

### กิจกรรมที่ 3 (ศึกษาเอกสารการสอนหน่วยที่ 5)

ใช้ตัวเลือกต่อไปนี้เติมลงหน้าข้อที่มีความหมายตรงกันให้ถูกต้อง

- |  |   |
|--|---|
| A. ภัยธรรมชาติ                           | B. ภัยคุกคามทางตรรกะ                        |
| C. ภัยคุกคามทางกายภาพ                    | D. ขอบเขตของการควบคุมทางกายภาพ              |
| E. มาตรการควบคุม                         | F. รายการตรวจสอบ                            |
| G. การวิเคราะห์ผลกระทบทางธุรกิจ          | H. แผนรับมือเหตุการณ์ฉุกเฉิน                |
| I. แผนกู้คืนระบบ                         | J. แผนดำเนินงานอย่างต่อเนื่อง               |
| K. ตัวอย่างคำถามที่ใช้ตรวจสอบสภาพแวดล้อม | L. ตัวอย่างคำถามที่ใช้ตรวจสอบการสำรองข้อมูล |

- \_\_\_ 1. กระบวนการเก็บข้อมูลสำรองมีการจัดลำดับความสำคัญอย่างไร
- \_\_\_ 2. ระบบไฟฟ้าสำรองฉุกเฉินสามารถทำงานได้นานเท่าใด
- \_\_\_ 3. การเตรียมความพร้อมให้กับหน่วยงานให้สามารถดำเนินภารกิจที่สำคัญได้หลังจากที่เกิดเหตุการณ์ฉุกเฉินหรือภัยพิบัติ
- \_\_\_ 4. การกำหนดรายละเอียดในการเตรียมการฟื้นฟูการดำเนินงานจากความเสียหายหรือภัยพิบัติที่ได้รับ
- \_\_\_ 5. การกำหนดรายละเอียดของกระบวนการและขั้นตอนที่ต้องดำเนินการเมื่อตรวจพบเหตุการณ์ฉุกเฉิน
- \_\_\_ 6. การระบุลำดับความสำคัญของความเสี่ยงที่จะต้องรีบดำเนินการแก้ไขโดยด่วน ระบุจุดล้มเหลวของระบบ และวิธีการรับมือกับปัญหา รวมถึงระบุผลกระทบที่มีต่อองค์กร
- \_\_\_ 7. เอกสารหรือรายการที่บันทึกเกี่ยวกับหัวข้อสำคัญที่จะต้องสอบถามหรือดำเนินการต่อไป
- \_\_\_ 8. แบ่งออกเป็น 3 ระดับ ได้แก่ ระดับที่ 1 พื้นที่ภายในอาณาเขต ระดับที่ 2 พื้นที่การเข้าถึงอาคาร และระดับที่ 3 พื้นที่ของศูนย์เทคโนโลยีสารสนเทศ
- \_\_\_ 9. ฮาร์ดแวร์หรือระบบเครือข่ายคอมพิวเตอร์ได้รับผลกระทบจากภัยคุกคามตามธรรมชาติหรือจากการกระทำของมนุษย์
- \_\_\_ 10. ระบบคอมพิวเตอร์ถูกผู้ไม่ประสงค์ดี ลักลอบเข้าถึงข้อมูลและทำการแก้ไขเปลี่ยนแปลงข้อมูลในระบบ



#### กิจกรรมที่ 4 (ศึกษาเอกสารการสอนหน่วยที่ 6)

จงใส่เครื่องหมายถูก (✓) หน้าข้อที่ถูกต้อง และใส่เครื่องหมายผิด (X) หน้าข้อที่ผิด

- \_\_\_ 1. การแข่งขันทางธุรกิจเป็นปัจจัยภายในที่เป็นแรงผลักดันและขับเคลื่อนต่อการตัดสินใจพัฒนาระบบสารสนเทศ
- \_\_\_ 2. การตรวจสอบนอกระบบ เป็นการใช่วิธีการทางคอมพิวเตอร์ช่วยในการตรวจสอบระบบสารสนเทศ
- \_\_\_ 3. หากมีการเพิ่มหรือขยายขอบเขตของโครงการ ต้องทำการประเมินค่าต้นทุนและเวลาดำเนินโครงการใหม่
- \_\_\_ 4. RAD เป็นการพัฒนาระบบสารสนเทศที่ใช้ระยะเวลาในการพัฒนาที่ค่อนข้างรวดเร็ว และมีการทำซ้ำในบางขั้นตอน
- \_\_\_ 5. การพัฒนาระบบโดยการสร้างต้นแบบ (prototyping) เป็นการสร้างระบบให้ผู้ใช้ทดลองใช้งาน เพื่อหาข้อบกพร่องและแก้ไขปรับปรุงแบบวนซ้ำไปเรื่อยๆ จนกว่าผู้ใช้จะยอมรับระบบทั้งหมดจึงนำไปใช้งาน
- \_\_\_ 6. การกำหนดและแบ่งแยกบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในโครงการทุกคน เป็นการควบคุมการบริหารโครงการ
- \_\_\_ 7. การควบคุมการทดสอบระบบสารสนเทศ ประกอบด้วย 2 ส่วน คือ การทดสอบโปรแกรม และการทดสอบระบบ
- \_\_\_ 8. การควบคุมการออกแบบส่วนนำเข้าข้อมูลของระบบสารสนเทศ ต้องกำหนดขั้นตอนการนำเข้าข้อมูล การตรวจทานข้อมูล การแก้ไขข้อมูล และการบันทึกข้อมูลที่ต้องการ
- \_\_\_ 9. การพบข้อผิดพลาดหรือปัญหาที่เกิดขึ้นจากระบบงานปัจจุบันเป็นปัจจัยภายนอกที่ส่งผลต่อการพัฒนาระบบสารสนเทศ
- \_\_\_ 10. การตรวจสอบผ่านระบบ เป็นการสอบถามความถูกต้องของข้อมูลที่ปรากฏในรายงานหรือเอกสาร โดยไม่สนใจว่าระบบทำการประมวลผลอย่างไร เหมาะกับการตรวจสอบรายการที่ไม่ซับซ้อนมากนัก



## กิจกรรมที่ 6 (ศึกษาเอกสารการสอนหน่วยที่ 9)

ใช้ตัวเลือกต่อไปนี้เติมลงหน้าข้อที่มีความหมายตรงกันให้ถูกต้อง

- |                                    |   |
|------------------------------------|---|
| A. ล็อกไฟล์ (log file)             | B. แชร์ล็อก (share lock)                  |
| C. การนิยามข้อมูล                  | D. พจนานุกรมข้อมูล                        |
| E. การสร้างวิว                     | F. จุดตรวจสอบ (check point)               |
| G. เดดล็อก (dead lock)             | H. ภาวะพร้อมกัน (concurrency)             |
| I. กฎควบคุมความถูกต้องของเอนทิตี   | J. กฎควบคุมความถูกต้องของการอ้างอิง       |
| K. ร่องรอยการตรวจสอบ (audit trail) | L. การสำรองข้อมูลเฉพาะที่มีการเปลี่ยนแปลง |

- \_\_\_ 1. ค่าของคีย์หลัก (Primary key) จะต้องไม่เป็นค่าว่าง
- \_\_\_ 2. ค่าของคีย์นอก (Foreign key) จะต้องสามารถอ้างอิงให้ตรงกับค่าของคีย์หลักได้หรือเป็นค่าว่างได้
- \_\_\_ 3. การบันทึกการเข้าสู่ระบบของผู้ใช้ ตั้งแต่เริ่มต้นเข้าสู่ระบบ จนกระทั่งออกจากระบบ โดยบันทึกว่าผู้ใช้เป็นใคร เข้าสู่ระบบจากที่ไหน กระทำการใดกับฐานข้อมูล และทำสำเร็จหรือไม่
- \_\_\_ 4. ทรานแซกชันที่มาทีหลังต้องรอทรานแซกชันที่มาก่อนคลายล็อกข้อมูล และทรานแซกชันที่มาก่อนก็ต้องรอทรานแซกชันที่มาทีหลังคลายล็อกข้อมูล
- \_\_\_ 5. ไฟล์ที่บันทึกการกระทำต่างๆ ของทรานแซกชันที่มีผลต่อการเปลี่ยนแปลงค่าของข้อมูลในฐานข้อมูล
- \_\_\_ 6. การใช้คำสั่งเอสคิวแอลเพื่อระบุรายละเอียดของโครงสร้างฐานข้อมูลหรือสคีมาที่ได้จากการออกแบบฐานข้อมูล
- \_\_\_ 7. ที่เก็บรายละเอียดต่างๆ ของข้อมูลภายในฐานข้อมูล รวมถึงคำอธิบายข้อมูลและความสัมพันธ์ระหว่างข้อมูล
- \_\_\_ 8. ผู้ใช้จะมองเห็นข้อมูลในมุมมองที่แตกต่างกัน โดยจะมองเห็นเฉพาะข้อมูลในส่วนของตนเองเกี่ยวข้องเท่านั้น
- \_\_\_ 9. ช่วงเวลา ณ ขณะใดขณะหนึ่งที่ระบบปฏิบัติการและระบบจัดการฐานข้อมูลนำข้อมูลของทรานแซกชันที่ดำเนินการสำเร็จเรียบร้อยแล้วจากที่เก็บข้อมูลชั่วคราวมาบันทึกลงในดิสก์
- \_\_\_ 10. ทรานแซกชันหลายๆ รายการ มีการใช้ข้อมูลเดียวกันร่วมกันในช่วงเวลาเดียวกัน

## กิจกรรมที่ 7 (ศึกษาเอกสารการสอนหน่วยที่ 10)

จงจับคู่ให้ถูกต้อง (โดยนำตัวเลือกด้านขวาไปเติมหน้าข้อด้านซ้ายที่มีความเกี่ยวข้องกัน)

- |   |  |
|---|--|
| ___ 1. การโจมตีที่พยายามแก้ไขเปลี่ยนแปลงทรัพยากรของระบบหรือส่งผลต่อการทำงานของระบบ  | A. การดักฟังแบบพาสซีฟ                  |
| ___ 2. การดักจับข้อมูลและนำไปดำเนินการต่อในนามของบุคคลอื่น  | B. การดักฟังแบบแอ็กทีฟ                 |
| ___ 3. ความพยายามทำให้เครื่องหรือทรัพยากรเครือข่ายสำหรับผู้ใช้งานเป้าหมายใช้บริการไม่ได้ เช่น ชัดขวางหรือชะลอบริการของแม่ข่ายที่เชื่อมโยงกับอินเทอร์เน็ตอย่างชั่วคราวหรือถาวร                       | C. การแย่งชิงเซสชัน                    |
| ___ 4. การโจมตีโดยการปลอมแปลงที่อยู่ต้นทางแล้วส่งคำร้องขอไปยังเครื่องคอมพิวเตอร์ทั้งหมดบนเครือข่าย ทำให้เครื่องคอมพิวเตอร์ทั้งหมดบนเครือข่ายตอบกลับมาจากจำนวนมากจนไม่สามารถสื่อสารกับเครื่องอื่นได้ | D. การปฏิเสธการให้บริการ (DoS)         |
| ___ 5. ชุดโพรโทคอลที่เป็นข้อตกลงเกี่ยวกับการรักษาความปลอดภัยในการส่งข้อมูลผ่านอินเทอร์เน็ต โดยใช้วิทยาการเข้ารหัสข้อมูล   | E. สเมอร์ฟ (Smurf)                     |
| ___ 6. การหลอกลวงทางอินเทอร์เน็ต โดยการส่งข้อความเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต ฯลฯ  | F. เครือข่ายแบบบัส                     |
| ___ 7. การควบคุมภัยคุกคามจากสัญญาณรบกวน   | G. เครือข่ายแบบดาว                     |
| ___ 8. ช่องโหว่ที่ปล่อยให้มินเครื่องเซิร์ฟเวอร์ เพื่อลวงให้แฮกเกอร์เข้ามาเจาะระบบเพื่อใช้สืบทัดตัวแฮกเกอร์และดักจับ   | H. เครือข่ายแบบวงแหวน                  |
| ___ 9. ผู้ใช้สามารถสั่งการหรือควบคุมเครื่องคอมพิวเตอร์ที่ให้บริการบนระบบเครือข่ายจากระยะไกลโดยการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่าน  | I. เครือข่ายแบบต้นไม้                  |
| ___ 10. การเชื่อมต่อเครือข่ายที่ทำให้การรับส่งข้อมูลต้องผ่านทุกเครื่องในทิศทางเดียวกัน แต่ละเครื่องจะตรวจสอบข้อมูลที่ส่งผ่านมา ถ้าไม่ใช่ของตนเองจะส่งผ่านไปยังเครื่องที่อยู่ลำดับถัดไป              | J. เครื่องทวนสัญญาณ (Repeater)         |
|   | K. SSH (Secure Shell)                  |
|   | L. การตรวจหาข้อผิดพลาดในระบบ           |
|   | M. ฮันนีพ็อต (Honey pot)               |
|   | N. อะพาเช่ (Apache)                    |
|   | O. ฟิชชิง (Phishing)                   |
|   | P. ใบรับรองดิจิทัล (CA)                |
|   | Q. การโจมตีแบบฟิงฟลัด (Ping flood)     |
|   | R. การโจมตีแบบซิงฟลัด (SYN flood)      |
|   | S. IIS (Internet Information Services) |
|   | T. เครือข่ายส่วนตัวเสมือน (VPN)        |
|   | U. ระบบตรวจจับการบุกรุก (IDS)          |
|   | V. ระบบป้องกันการบุกรุก (IPS)          |
|   | W. การเข้ารหัสแบบ WEP                  |
|   | X. การเข้ารหัสแบบ WPA                  |
|   | Y. SSID (Service Set Identifier)       |
|   | Z. IPsec (Internet Protocol Security)  |





