กิจกรรมประจำชุดวิชา 96404
การตรวจสอบระบบงานคอมพิวเตอรและการควบคุมภายใน
ภาคปลาย ปีการศึกษา 2568
สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

คำนำ

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

การประเมินกิจกรรม เป็นส่วนหนึ่งของการวัดผลสัมฤทธิ์ทางการเรียนสุดท้าย จึงกำหนดให้นักศึกษาทำกิจกรรมภาคปฏิบัติตามที่กำหนดให้ โดยมีวัตถุประสงค์เพื่อให้นักศึกษามีความสามารถ ดังนี้

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

นอกจากนี้การทำกิจกรรมประจำชุดวิชายังทำให้นักศึกษาได้ศึกษาเอกสารการสอนตั้งแต่ต้นภาคการศึกษา และจากการวิจัยพบว่านักศึกษาที่ทำกิจกรรมจะมีโอกาสสอบผ่านในปลายภาคมากกว่านักศึกษาที่ไม่ทำกิจกรรม

คณะกรรมการบริหารชุดวิชาการตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน ขอให้นักศึกษาทุกท่านประสบความสำเร็จในการศึกษาชุดวิชานี้ และสามารถนำความรู้ไปเป็นประโยชน์ต่อการดำเนินชีวิตและการประกอบอาชีพสืบไป

คณะกรรมการบริหารชุดวิชาการตรวจสอบระบบงานคอมพิวเตอร์
และการควบคุมภายใน

1. การประเมินผล

เกณฑ์การให้คะแนนกิจกรรมจะพิจารณาจากการตอบที่ตรงประเด็นคำถาม การครอบคลุมความถูกต้องของคำตอบ ความชัดเจนของการนำเสนอ ความละเอียดประณีตของชิ้นงาน

มหาวิทยาลัยไม่บังคับให้นักศึกษาทุกคนต้องทำกิจกรรม นักศึกษาอาจเลือกทำหรือไม่ทำก็ได้ โดยการประเมินผลปลายภาคสำหรับชุดวิชานี้ แบ่งออกเป็น 2 กรณี

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

กรณีที่ 2 นักศึกษาไม่ทำกิจกรรม มหาวิทยาลัยจะประเมินผลจากการสอบปลายภาคเพียงอย่างเดียว

ในการประเมินผลสอบปลายภาค นักศึกษาทั้งกลุ่มที่ทำกิจกรรมและไม่ทำกิจกรรม จะได้รับการประเมินผลโดยใช้ข้อสอบฉบับเดียวกัน นักศึกษากลุ่มที่ทำกิจกรรมมีคะแนนเต็ม 80 คะแนน ส่วนนักศึกษากลุ่มที่ไม่ทำกิจกรรมมีคะแนนเต็ม 100 คะแนน

สำหรับนักศึกษาที่ทำกิจกรรมมหาวิทยาลัยจะพิจารณาให้นักศึกษาได้ประโยชน์สูงสุด โดยการนำคะแนนสอบปลายภาคของนักศึกษาเพียงอย่างเดียวมาเปรียบเทียบกับการคิดคะแนนสอบปลายภาครวมกับคะแนนกิจกรรม แล้วนำคะแนนส่วนที่มากกว่าไปใช้ในการตัดสินผลการสอบให้กับนักศึกษา ดังตัวอย่างต่อไปนี้

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

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

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

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

มหาวิทยาลัยจะเลือกให้นักศึกษาได้คะแนน 62.50 คะแนน นั่นคือ *สอบผ่าน*

2. การส่งกิจกรรมประจำชุดวิชา

ให้นักศึกษาดำเนินการดังนี้

1. ให้นักศึกษาสงกิจกรรมประจำชุดวิชาภายใน **วันที่ 30 เมษายน 2569**
2. ให้จัดทำหน้าปกรายงานให้มีข้อความตามตัวอย่าง หรือใช้หน้าปกรายงานตามที่แนบไว้ตอนท้าย
3. ให้**ส่งกิจกรรมประจำชุดวิชา**ทางช่องทางใดช่องทางหนึ่ง ดังนี้
   - ส่งด้วยตนเอง ณ สำนักบริการการศึกษา มหาวิทยาลัยสุโขทัยธรรมาธิราช
   - ส่งผ่านช่องทางออนไลน์ที่เว็บไซต์ https://eduapp.stou.ac.th/practice/
   - ส่งทางไปรษณีย์ลงทะเบียน โดยจ่าหน้าซองดังนี้

ศูนย์บริการการสอนทางไปรษณีย์
สำนักบริการการศึกษา
มหาวิทยาลัยสุโขทัยธรรมาธิราช
ตำบลบางพูด อำเภอปากเกร็ด
จังหวัดนนทบุรี 11120

(กิจกรรมประจำชุดวิชา 96404
การตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน
สาขาวิชาวิทยาศาสตร์และเทคโนโลยี)

4. ให้นักศึกษา **แสดงวิธีการหาคำตอบ** ของโจทย์ในกิจกรรม โดย **เขียนด้วยลายมือตนเอง เท่านั้น ให้นักศึกษาทำกิจกรรมด้วยตนเอง *<u>ถ้าตรวจสอบได้ว่ามีการลอกกัน หรือไม่ได้ใช้ความรู้ของตนเอง หรือวิธีทำเหมือนกันหลายฉบับ จะไม่ตรวจให้คะแนน</u>***

   การเขียนด้วยลายมือตัวเองนั้นนักศึกษาอาจเขียนลงกระดาษแล้วถ่ายรูป หรือใช้ปากกาดิจิทัลเขียนบน pad และ save เป็นไฟล์รูปภาพ หรือ ไฟล์ pdf

ในกรณีที่ส่งกิจกรรมทางไปรษณีย์ ให้เก็บสลิปหรือต้นขั้วการส่ง และถ่ายเอกสารกิจกรรมทั้งหมดไว้เป็นหลักฐาน

นักศึกษาสามารถตรวจสอบว่าสำนักบริการการศึกษาได้รับกิจกรรมที่นักศึกษาส่งไปแล้วหรือยัง โดยโทรศัพท์สอบถามที่หมายเลข 0-2982-9633 หรือโทรศัพท์ติดต่อสำนักบริการการศึกษา หมายเลข 0-2-504-7621 หรือโทรศัพท์ติดต่อศูนย์สารสนเทศ หมายเลข 0-2504-7788 หรือ e-mail : ic.proffice@stou.ac.th

ปกรายงาน

กิจกรรมประจำชุดวิชา 96404

การตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ภาคปลาย ปีการศึกษา 2568

ชื่อนักศึกษา.....

รหัสประจำตัวนักศึกษา | | | | | | | | | | |

ที่อยู่ .....

.....

โทรศัพท์ (ถ้ามี) .....

ข้าพเจ้าขอยอมรับการตัดสินผลคะแนนการทำกิจกรรมประจำชุดวิชา
จากผู้ประเมินถือเป็นที่สิ้นสุด

ลงชื่อ.....

(.....)

3. เนื้อหากิจกรรม

<u>คำชี้แจง</u> กิจกรรมมีทั้งหมด 15 กิจกรรม คิดเป็นคะแนนรวมทั้งหมด 20 คะแนน
ให้นักศึกษา**ทำกิจกรรมทุกข้อ** ลงในเอกสารกิจกรรมประจำชุดวิชาฉบับนี้เท่านั้น
โดย**เขียนตอบด้วยลายมือตนเองเท่านั้น**

กิจกรรมที่ 1 (ศึกษาเอกสารการสอน**หน่วยที่ 1)**

จงจับคู่ให้ถูกต้อง (โดยนำตัวอักษรที่อยู่หน้าตัวเลือกด้านขวา เติมลงหน้าข้อด้านซ้ายที่มีความเกี่ยวข้องกัน)

____ 1. วัตถุประสงค์ของการควบคุมเทคโนโลยีสารสนเทศ ได้แก่ เพื่อรักษาความลับ เพื่อรักษาความครบถ้วนถูกต้อง และเพื่อรักษาสภาพพร้อมใช้งาน
____ 2. คุณลักษณะที่พึงประสงค์ของระบบราชการไทย 8 ประการ
____ 3. หลักการกระจายอำนาจและหลักการมีส่วนร่วม/การมุ่งเน้นฉันทามติ
____ 4. ตัว R ในหลักธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT GRC)
____ 5. ขั้นตอนของการตรวจสอบเทคโนโลยีสารสนเทศในช่วงวางแผนการตรวจสอบ
____ 6. การตรวจสอบการควบคุมข้อมูลนำเข้า การตรวจสอบการควบคุมการประมวลผล และการตรวจสอบการควบคุมผลลัพธ์
____ 7. ประเภทของการควบคุม 3 ระดับ ได้แก่ การควบคุมเพื่อป้องกัน การควบคุมเพื่อค้นหา และการควบคุมเพื่อแก้ไข
____ 8. คำสั่งซื้อของลูกค้าทุกรายการต้องผ่านการอนุมัติจากผู้จัดการฝ่ายขาย ทำให้การจัดส่งสินค้าให้ลูกค้าเกิดความล่าช้า
____ 9. แนวทางที่ได้รับการรับรองจากสมาคมผู้ตรวจสอบภายในสากล และผ่านการพิจารณาอนุมัติอย่างเป็นทางการ เพื่อใช้อธิบายถึงวิธีการปฏิบัติตามมาตรฐานสากลในการปฏิบัติงานวิชาชีพตรวจสอบภายในและประมวลจรรยาบรรณ
____ 10. บุคคลภายนอกองค์กรที่ได้รับการติดต่อให้ทำหน้าที่ตรวจสอบองค์กร และแสดงความคิดเห็นเกี่ยวกับการควบคุมภายในขององค์กร

A. ผู้ตรวจสอบภายใน
B. ผู้ตรวจสอบภายนอก
C. แนวทางภาคบังคับ
D. แนวทางที่แนะนำให้นำไปใช้
E. คอขวดในกระบวนการทำงาน
F. แบบจำลองการควบคุม PDC
G. การตรวจสอบการควบคุมทั่วไป
H. การตรวจสอบการควบคุมระบบงานประยุกต์
I. การตรวจสอบการควบคุมสื่อสังคม
J. ศึกษาโครงสร้างองค์กรและสำรวจข้อมูลเบื้องต้น
K. ตัดขั้นตอนการทำงานที่ไม่เพิ่มมูลค่า
L. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
M. การควบคุมที่เกินความจำเป็น
N. การปฏิบัติตามมาตรฐานการให้บริการ
O. ประชารัฐ
P. I AM READY
Q. IPPF
R. CIA

กิจกรรมที่ 2 (ศึกษาเอกสารการสอน**หน่วยที่ 2)**

จงจับคู่ให้ถูกต้อง (โดยนำตัวอักษรที่อยู่หน้าตัวเลือกด้านขวา เติมลงหน้าข้อด้านซ้ายที่มีความเกี่ยวข้องกัน)

_____ 1. ความเสี่ยงที่ผู้บริหารควรให้ความสำคัญมากที่สุด

_____ 2. วิธีการประเมินตนเองที่ขยายผลต่อจากการประเมินตนเองเกี่ยวกับความเสี่ยงและการควบคุม โดยเพิ่มการพิจารณาว่ากระบวนการนั้นได้ดำเนินการเพื่อที่จะบรรลุความต้องการของลูกค้าและผู้มีส่วนได้ส่วนเสียที่สำคัญขององค์กร

_____ 3. มี 3 วิธี ได้แก่ การประเมินร่วมกัน การสัมภาษณ์ผู้ประเมินโดยตรง และการสำรวจ

_____ 4. การกำหนดให้พนักงานขายสามารถกำหนดและอนุมัติวงเงินเครดิตให้แก่ลูกค้าในระบบขายหรือระบบลูกหนี้ได้

_____ 5. เครื่องคอมพิวเตอร์ขัดข้องเนื่องจากขนาดพื้นที่ในการจัดเก็บข้อมูลมีเนื้อที่เหลือไม่เพียงพอ

_____ 6. ขั้นตอนแรกของการบริหารความเสี่ยงด้านเทคโนโลยี-สารสนเทศ

_____ 7. กำหนดสิทธิผู้ใช้ไม่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

_____ 8. ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตเข้าสู่ระบบเทคโนโลยีสารสนเทศขององค์กร

_____ 9. การทำประกันอัคคีภัย เพื่อให้ได้รับการชดเชยค่าเสียหายในกรณีที่เกิดไฟไหม้ศูนย์คอมพิวเตอร์

_____ 10. ประกอบด้วย 3 ขั้นตอน ได้แก่ การระบุประเภทของความเสี่ยง การระบุสาเหตุที่ทำให้เกิดความเสี่ยง และการวิเคราะห์ความเสี่ยง

A. การระบุทรัพย์สินเทคโนโลยีสารสนเทศ
B. การระบุสาเหตุที่ทำให้เกิดความเสี่ยง
C. การลดโอกาสที่จะเกิดความเสี่ยง
D. การโอนความเสี่ยง
E. การประเมินความเสี่ยง
F. การวิเคราะห์ความเสี่ยง
G. การระบุประเภทความเสี่ยง
H. การกำหนดสิทธิการเข้าถึงในระดับฟิลด์ไม่เหมาะสม
I. การกำหนดสิทธิในระดับหน้าที่งานไม่เหมาะสม
J. การหยุดชะงักของการประมวลผล
K. การหยุดชะงักของการติดต่อสื่อสาร
L. เทคนิคที่ใช้ในการประเมินตนเอง
M. ข้อจำกัดของการประเมินตนเอง
N. ประโยชน์ของการประเมินตนเอง
O. การประเมินตนเองเกี่ยวกับความเสี่ยง การควบคุม และผลการปฏิบัติงาน
P. ความเสี่ยงระดับที่ 1
Q. ความเสี่ยงระดับที่ 2
R. ความเสี่ยงระดับที่ 3
S. ความเสี่ยงระดับที่ 4

กิจกรรมที่ 3 (ศึกษาเอกสารการสอน**หน่วยที่ 3**)

จงลากเส้นเชื่อมโยงความสัมพันธ์ที่เกี่ยวข้องกันของ**หลักการ COSO** ให้ถูกต้อง

การประเมินความเสี่ยง	○	○	กำหนดนโยบายและวิธีปฏิบัติ สอบทานโดยผู้บริหาร แบ่งแยกหน้าที่ ควบคุมการประมวลผลและกายภาพ
การตอบสนองต่อความเสี่ยง	○	○	เผยแพร่ประชาสัมพันธ์และชี้แจงวัตถุประสงค์ให้บุคลากรทุกระดับทราบและเข้าใจทิศทางเดียวกัน
การกำหนดกิจกรรมการควบคุม	○	○	ระบุปัจจัยเสี่ยง วิเคราะห์ความเสี่ยง และบริหารความเสี่ยง
การนำไปใช้ในทุกระดับขององค์กร	○	○	หลีกเลี่ยงความเสี่ยง ควบคุมความเสี่ยง หาผู้ร่วม-รับผิดชอบความเสี่ยง และยอมรับความเสี่ยง

จงลากเส้นเชื่อมโยงความสัมพันธ์ที่เกี่ยวข้องกันของ**หลักการ CobiT 5** ให้ถูกต้อง

APO	○	○	การวัดผล สั่งการ และเฝ้าติดตาม
BAI	○	○	การส่งมอบ ให้บริการ และสนับสนุน
EDM	○	○	การเฝ้าติดตาม วัดผล และประเมิน
DSS	○	○	การวางแนว ทำแผน และจัดระบบ
MEA	○	○	การสร้าง จัดหา และนำไปใช้

จงลากเส้นเชื่อมโยงความสัมพันธ์ที่เกี่ยวข้องกันของ**หลักการ ITIL** ให้ถูกต้อง

SD	○	○	การส่งมอบงานบริการ ได้แก่ การจัดการการเปลี่ยนแปลง การจัดการคุณสมบัติของอุปกรณ์และทรัพย์สินที่ให้บริการ การจัดการความรู้ การวางแผนและสนับสนุนการส่งมอบ การตรวจสอบและทดสอบงานบริการ การจัดการนำบริการใหม่ไปใช้ และการประเมินผลการเปลี่ยนแปลง
SO	○		
CSI	○	○	การปฏิบัติงานบริการให้เป็นไปตามข้อตกลงระดับการให้บริการ (SLA)
		○	การปรับปรุงงานบริการให้ดีขึ้นอย่างต่อเนื่อง โดใช้แนวคิด PDCA
SS	○	○	กลยุทธ์ของการบริการ ได้แก่ การจัดการเชิงกลยุทธ์ การจัดการรายการบริการ การจัดการทางการเงิน การจัดการความต้องการ และการจัดการความสัมพันธ์ทางธุรกิจ
ST	○	○	การออกแบบงานบริการ ได้แก่ การประสานงานออกแบบ การจัดการรายการบริการ การจัดการระดับการบริการ การจัดการความพร้อมใช้ การจัดการสมรรถนะ การจัดการความต่อเนื่องในการให้บริการ การจัดการความมั่นคงปลอดภัย และการจัดการผู้แทนจำหน่าย

กิจกรรมที่ 4 (ศึกษาเอกสารการสอน**หน่วยที่ 4)**

4.1 จงบอกลักษณะความเป็นผู้นำของผู้บริหารส่วนงานเทคโนโลยีสารสนเทศ

.....

.....

.....

.....

.....

.....

.....

4.2 จงบอกแนวทางการควบคุมด้านการพัฒนาบุคลากรในส่วนงานเทคโนโลยีสารสนเทศ มาพอสังเขป

.....

.....

.....

.....

.....

.....

.....

4.3 จงสรุปแนวทางการตรวจสอบมาตรฐานการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มาพอสังเขป

.....

.....

.....

.....

.....

.....

.....

.....

กิจกรรมที่ 5 (ศึกษาเอกสารการสอน**หน่วยที่ 5)**

ใช้ตัวเลือกต่อไปนี้เติมลงหน้าข้อที่มีความหมายตรงกันให้ถูกต้อง

A. แผนกู้คืนระบบ
B. แผนดำเนินงานอย่างต่อเนื่อง
C. แผนรับมือเหตุการณ์ฉุกเฉิน
D. การวิเคราะห์ผลกระทบทางธุรกิจ
E. รายการตรวจสอบ
F. มาตรการควบคุม
G. ภัยคุกคามทางตรรกะ
H. ภัยคุกคามทางกายภาพ
I. ขอบเขตของการควบคุมทางกายภาพ
J. ความถี่ในการตรวจสอบทางกายภาพ
K. กระบวนการตรวจสอบสภาพแวดล้อม
L. กระบวนการตรวจสอบการสำรองและกู้คืนข้อมูล

____1. เอกสารหรือรายการที่บันทึกเกี่ยวกับหัวข้อสำคัญที่จะต้องสอบถามหรือดำเนินการต่อไป

____2. การระบุลำดับความสำคัญของความเสี่ยงที่จะต้องรีบดำเนินการแก้ไขโดยด่วน ระบุจุดล้มเหลวของระบบและวิธีการรับมือกับปัญหา รวมถึงระบุผลกระทบที่มีต่อองค์กร

____3. การกำหนดรายละเอียดของกระบวนการและขั้นตอนที่ต้องดำเนินการเมื่อตรวจพบเหตุการณ์ฉุกเฉิน

____4. การเตรียมความพร้อมให้กับหน่วยงานให้สามารถดำเนินภารกิจที่สำคัญได้หลังจากที่เกิดเหตุการณ์ฉุกเฉินหรือภัยพิบัติ

____5. การกำหนดรายละเอียดในการเตรียมการฟื้นฟูการดำเนินงานจากความเสียหายหรือภัยพิบัติที่ได้รับ

____6. ระบบคอมพิวเตอร์ถูกผู้ไม่ประสงค์ดีลักลอบเข้าถึงข้อมูลและทำการแก้ไขเปลี่ยนแปลงข้อมูลในระบบ

____7. ฮาร์ดแวร์หรือระบบเครือข่ายคอมพิวเตอร์ได้รับความเสียหายจากไฟไหม้

____8. แบ่งออกเป็น 3 ระดับ ได้แก่ ระดับที่ 1 พื้นที่ภายในอาณาเขต ระดับที่ 2 พื้นที่การเข้าถึงอาคาร และระดับที่ 3 พื้นที่ของศูนย์เทคโนโลยีสารสนเทศ

____9. ระบบไฟฟ้าสำรองฉุกเฉินสามารถทำงานได้นานเท่าใด

____10. กระบวนการเก็บข้อมูลสำรองมีการจัดลำดับความสำคัญอย่างไร

กิจกรรมที่ 6 (ศึกษาเอกสารการสอน**หน่วยที่ 6)**

จงใส่เครื่องหมายถูก (✓) หน้าข้อที่ถูกต้อง และใส่เครื่องหมายผิด (X) หน้าข้อที่ผิด

____1. หากมีการเพิ่มหรือขยายขอบเขตของโครงการ ต้องทำการประเมินค่าต้นทุนและเวลาดำเนินโครงการใหม่

____2. RAD เป็นการพัฒนาระบบสารสนเทศที่ใช้ระยะเวลาในการพัฒนาที่ค่อนข้างรวดเร็ว และมีการทำซ้ำในบางขั้นตอน

____3. การพัฒนาระบบโดยการสร้างต้นแบบ (prototyping) เป็นการสร้างระบบให้ผู้ใช้ทดลองใช้งาน เพื่อหาข้อบกพร่องและแก้ไขปรับปรุงแบบวนซ้ำไปเรื่อยๆ จนกว่าผู้ใช้จะยอมรับระบบทั้งหมดจึงนำไปใช้งาน

____4. การกำหนดและแบ่งแยกบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในโครงการทุกคนเป็นการควบคุมการบริหารโครงการ

____5. การควบคุมการทดสอบระบบสารสนเทศ ประกอบด้วย 2 ส่วน คือ การทดสอบโปรแกรม และการทดสอบระบบ

____6. การควบคุมการออกแบบส่วนนำเข้าข้อมูลของระบบสารสนเทศ ต้องกำหนดขั้นตอนการนำเข้าข้อมูล การตรวจทานข้อมูล การแก้ไขข้อมูล และการบันทึกข้อมูลที่ถูกต้อง

____7. การแข่งขันทางธุรกิจเป็นปัจจัยภายในที่เป็นแรงผลักดันและขับเคลื่อนต่อการตัดสินใจพัฒนาระบบสารสนเทศ

____8. การพบข้อผิดพลาดหรือปัญหาที่เกิดขึ้นจากระบบงานปัจจุบันเป็นปัจจัยภายนอกที่ส่งผลต่อการพัฒนาระบบสารสนเทศ

____9. การตรวจสอบนอกระบบ เป็นการใช้วิธีการทางคอมพิวเตอร์ช่วยในการตรวจสอบระบบสารสนเทศ

____10. การตรวจสอบผ่านระบบ เป็นการสอบทานความถูกต้องของข้อมูลที่ปรากฏในรายงานหรือเอกสาร โดยไม่สนใจว่าระบบทำการประมวลผลอย่างไร เหมาะกับการตรวจสอบรายการที่ไม่ซับซ้อนมากนัก

กิจกรรมที่ 7 (ศึกษาเอกสารการสอน**หน่วยที่ 7)**

จงจับคู่ให้ถูกต้อง (โดยนำตัวอักษรที่อยู่หน้าตัวเลือกด้านขวา เติมลงหน้าข้อด้านซ้ายที่มีความเกี่ยวข้องกัน)

_____ 1. ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง

_____ 2. การบริหารจัดการเทคนิคและกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูลให้เป็นมาตรฐาน

_____ 3. การจัดทำบัญชีทรัพย์สิน ระบุผู้เป็นเจ้าของทรัพย์สิน การใช้และการคืนทรัพย์สินอย่างเหมาะสม

_____ 4. กำหนดบทลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดระเบียบปฏิบัติด้านความมั่นคงปลอดภัยขององค์กร

_____ 5. จัดทำนโยบายด้านความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร และเผยแพร่ให้บุคลากรที่เกี่ยวข้องได้รับทราบ

_____ 6. ตรวจสอบแผนผังโครงสร้างองค์กรของส่วนงานเทคโนโลยีสารสนเทศและหน่วยงานควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

_____ 7. การกำหนดสิทธิในการเข้าถึงระบบเครือข่ายโดยต้องพิสูจน์ยืนยันตัวตนก่อนเข้าใช้งาน เพื่อเป็นการป้องกันการเข้าถึงบริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

_____ 8. การทำให้มั่นใจว่า สารสนเทศอยู่ในสภาพที่พร้อมจะให้บริการได้ตลอดเวลา ระบบมีความเสถียร มีแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติที่เชื่อถือได้

_____ 9. การทำให้มั่นใจว่า สารสนเทศจะได้รับการบันทึกและแก้ไขปรับปรุง โดยบุคคลหรือวิธีการที่ถูกต้องและได้รับอนุญาต

_____ 10. การทำให้มั่นใจว่า สารสนเทศที่เก็บรักษาไว้จะมีเพียงบุคคลที่ได้รับอนุญาตที่แท้จริงเท่านั้น จึงจะสามารถเข้าถึงได้

A. การรักษาความลับ (C)

B. การรักษาความครบถ้วนสมบูรณ์ (I)

C. การรักษาสภาพพร้อมใช้งาน (A)

D. ความมั่นคงปลอดภัยของคอมพิวเตอร์และข้อมูล

E. ความมั่นคงปลอดภัยของเครือข่าย

F. นโยบายความมั่นคงปลอดภัยขององค์กร

G. การตรวจสอบความมั่นคงปลอดภัยสารสนเทศทางกายภาพ

H. การตรวจสอบความมั่นคงปลอดภัยสารสนเทศทางตรรกะ

I. A.5 การกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

J. A.7 ความมั่นคงปลอดภัยสารสนเทศด้านทรัพยากรมนุษย์

K. A.8 การบริหารจัดการทรัพย์สินองค์กร3

L. A.10 การเข้ารหัสข้อมูล

M. A.12 ความปลอดภัยในการปฏิบัติงาน

N. CISO

กิจกรรมที่ 8 (ศึกษาเอกสารการสอน**หน่วยที่ 8**)

8.1 จงบอกจุดประสงค์ของการนำรหัสมาใช้ในการนำเข้าข้อมูล

.....

.....

.....

.....

8.2 จงบอกลักษณะของข้อมูลที่ไม่ควรนำเข้าเพื่อประมวลผล

.....

.....

.....

.....

.....

8.3 จงบอกสาเหตุที่ทำให้เกิดข้อผิดพลาดในการประมวลผล

.....

.....

.....

.....

.....

.....

.....

.....

8.4 จงบอกแนวทางในการควบคุมผลลัพธ์ มาพอสังเขป

.....

.....

.....

.....

.....

.....

.....

.....

กิจกรรมที่ 9 (ศึกษาเอกสารการสอน**หน่วยที่ 9)**

ใช้ตัวเลือกต่อไปนี้เติมลงหน้าข้อที่มีความหมายตรงกันให้ถูกต้อง

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

____1. การบันทึกการเข้าสู่ระบบของผู้ใช้ ตั้งแต่เริ่มต้นเข้าสู่ระบบ จนกระทั่งออกจากระบบ โดยบันทึกว่าผู้ใช้เป็นใคร เข้าสู่ระบบจากที่ไหน กระทำการใดกับฐานข้อมูล และทำสำเร็จหรือไม่

____2. ค่าของคีย์นอก (foreign key) จะต้องสามารถอ้างอิงให้ตรงกับค่าของคีย์หลักได้หรือเป็นค่าว่างได้

____3. ค่าของคีย์หลัก (primary key) จะต้องไม่เป็นค่าว่าง

____4. ทรานแซกชันที่มาทีหลังต้องรอทรานแซกชันที่มาก่อนทำการคลายล็อคข้อมูล และทรานแซกชันที่มาก่อนก็ต้องรอทรานแซกชันที่มาทีหลังทำการคลายล็อคข้อมูล

____5. ไฟล์ที่บันทึกการกระทำต่างๆ ของทรานแซกชันที่มีผลต่อการเปลี่ยนแปลงค่าของข้อมูลในฐานข้อมูล

____6. ทรานแซกชันหลายๆ รายการ มีการใช้ข้อมูลเดียวกันร่วมกันในช่วงเวลาเดียวกัน

____7. ผู้ใช้จะมองเห็นข้อมูลในมุมมองที่แตกต่างกัน โดยจะมองเห็นเฉพาะข้อมูลในส่วนที่ตนเองเกี่ยวข้องเท่านั้น

____8. การใช้คำสั่งเอสคิวแอลเพื่อสร้างโครงสร้างฐานข้อมูลหรือสคีมาที่ได้จากการออกแบบฐานข้อมูล

____9. ที่เก็บรายละเอียดต่างๆ ของข้อมูลภายในฐานข้อมูล รวมถึงคำอธิบายข้อมูลและความสัมพันธ์ระหว่างข้อมูล

____10. ช่วงเวลา ณ ขณะใดขณะหนึ่งที่ระบบปฏิบัติการและระบบจัดการฐานข้อมูลนำข้อมูลของทรานแซกชันที่ทำสำเร็จเรียบร้อยแล้วจากที่เก็บข้อมูลชั่วคราวมาบันทึกลงในดิสก์

กิจกรรมที่ 10 (ศึกษาเอกสารการสอน**หน่วยที่ 10)**

จงจับคู่ให้ถูกต้อง (โดยนำตัวอักษรที่อยู่หน้าตัวเลือกด้านขวา เติมลงหน้าข้อด้านซ้ายที่มีความเกี่ยวข้องกัน)

____ 1. การโจมตีโดยการปลอมแปลงที่อยู่ต้นทางแล้วส่งคำร้องขอไปยังเครื่องคอมพิวเตอร์ทั้งหมดบนเครือข่าย ทำให้เครื่องคอมพิวเตอร์ทั้งหมดบนเครือข่ายตอบกลับมาจำนวนมากจนไม่สามารถสื่อสารกับเครื่องอื่นได้

____ 2. ความพยายามทำให้เครื่องหรือทรัพยากรเครือข่ายสำหรับผู้ใช้เป้าหมายใช้บริการไม่ได้ เช่น ขัดขวางหรือชะลอบริการของแม่ข่ายที่เชื่อมโยงกับอินเทอร์เน็ตอย่างชั่วคราวหรือถาวร

____ 3. การดักจับข้อมูลและนำไปดำเนินการต่อในนามของบุคคลอื่น

____ 4. การโจมตีที่พยายามแก้ไขเปลี่ยนทรัพยากรของระบบหรือส่งผลต่อการทำงานของระบบ

____ 5. ชุดโพรโทคอลที่เป็นข้อตกลงเกี่ยวกับการรักษาความปลอดภัยในการส่งข้อมูลผ่านอินเทอร์เน็ต โดยใช้วิทยาการการเข้ารหัสข้อมูล

____ 6. การหลอกลวงทางอินเทอร์เน็ต โดยการส่งข้อความเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต ฯลฯ

____ 7. ช่องโหว่ที่ปล่อยให้มีบนเครื่องเซิร์ฟเวอร์ เพื่อลวงให้แฮกเกอร์เข้ามาเจาะระบบเพื่อใช้สืบหาตัวแฮกเกอร์และดักจับ

____ 8. การควบคุมภัยคุกคามจากสัญญาณรบกวน

____ 9. ผู้ใช้สามารถสั่งการหรือควบคุมเครื่องคอมพิวเตอร์ที่ให้บริการบนระบบเครือข่ายจากระยะไกลโดยการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่าน

____ 10. การเชื่อมต่อเครือข่ายที่ทำให้การรับส่งข้อมูลต้องผ่านทุกเครื่องในทิศทางเดียวกัน แต่ละเครื่องจะตรวจสอบข้อมูลที่ส่งผ่านมา ถ้าไม่ใช่ของตนเองจะส่งผ่านไปยังเครื่องที่อยู่ลำดับถัดไป

A. การดักฟังแบบพาสซีฟ
B. การดักฟังแบบแอ็กทีฟ
C. การแย่งชิงเซสชัน
D. การปฏิเสธการให้บริการ (DoS)
E. สเมิร์ฟ (smurf)
F. เครือข่ายแบบบัส
G. เครือข่ายแบบดาว
H. เครือข่ายแบบวงแหวน
I. เครือข่ายแบบต้นไม้
J. เครื่องทวนสัญญาณ (repeater)
K. SSH (Secure Shell)
L. การตรวจหาข้อผิดพลาดในระบบ
M. ฮันนีพ็อต (honey pot)
N. อะพาเช่ (Apache)
O. ฟิชชิ่ง (Phishing)
P. ใบรับรองฝั่งเซิร์ฟเวอร์ (CA)
Q. การโจมตีแบบพิงฟลัด (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)

กิจกรรมที่ 11 (ศึกษาเอกสารการสอน**หน่วยที่ 11)**

11.1 ช่องโหว่ของโปรแกรมประยุกต์บนเว็บที่พบโดยทั่วไป มีอะไรบ้าง

.....

.....

.....

.....

.....

.....

.....

.....

11.2 จงบอกวิธีการควบคุมการถูกแทรกสคริป์ลงในหน้าเว็บเพจ

.....

.....

.....

.....

.....

.....

.....

11.3 จงสรุปการตรวจสอบเอพีไอ มาพอสังเขป

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

กิจกรรมที่ 12 (ศึกษาเอกสารการสอน**หน่วยที่ 12)**

12.1 จงสรุปแนวทางการควบคุมระบบสารสนเทศบนเครือข่ายอินเทอร์เน็ต

.....

.....

.....

.....

.....

.....

.....

.....

12.2 จงยกตัวอย่างระบบผู้เชี่ยวชาญที่ใช้ในการตรวจสอบ

.....

.....

.....

.....

.....

.....

.....

12.3 จงสรุปแนวทางการควบคุมและตรวจสอบการใช้บริการเทคโนโลยีสารสนเทศจากภายนอก มาพอสังเขป

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

กิจกรรมที่ 13 (ศึกษาเอกสารการสอน**หน่วยที่ 13)**

13.1 จงลากเส้นเชื่อมโยงความสัมพันธ์ของสื่อสังคมในแต่ละกลุ่ม ให้ถูกต้อง

LinkedIn	○	○	กลุ่มสื่อสังคมการพูดคุย
Pinterest	○	○	กลุ่มสื่อสังคมใช้งานทั่วไป
Line	○	○	กลุ่มสื่อสังคมการแชร์ภาพและวิดีโอ
Facebook	○	○	กลุ่มสื่อสังคมช่วยในการทำงาน
Instagram	○	○	กลุ่มสื่อสังคมที่มีความสนใจและความชอบเหมือนกัน

13.2 ในการประเมินสื่อสังคมขององค์กร จะทำการประเมิน 6 ด้าน มีอะไรบ้าง จงอธิบายพอสังเขป

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

13.3 รายงานผู้เข้าใช้สื่อสังคม แบ่งออกเป็น 4 ประเภท อะไรบ้าง จงอธิบายพอสังเขป

.....

.....

.....

.....

.....

.....

.....

.....

.....

กิจกรรมที่ 14 (ศึกษาเอกสารการสอน**หน่วยที่ 14)**

14.1 ขั้นตอนการนำซอฟต์แวร์ทั่วไปมาใช้ในการตรวจสอบมีกี่ขั้นตอน อะไรบ้าง จงอธิบายพอสังเขป

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

14.2 จงอธิบายซอฟต์แวร์อรรถประโยชน์ต่อไปนี้ มาพอสังเขป

1) ด้านการรักษาความปลอดภัย .....

.....

.....

.....

2) ด้านการอำนวยความสะดวก .....

.....

.....

.....

3) ด้านการประเมินคุณภาพของข้อมูล .....

.....

.....

.....

4) ด้านการประเมินประสิทธิภาพของการทำงาน .....

.....

.....

.....

กิจกรรมที่ 15 (ศึกษาเอกสารการสอน**หน่วยที่ 15)**

จงจับคู่ให้ถูกต้อง (โดยนำตัวอักษรที่อยู่หน้าตัวเลือกด้านขวา เติมลงหน้าข้อด้านซ้ายที่มีความเกี่ยวข้องกัน)

____ 1. การกระทำของนักพัฒนาโปรแกรม โดยเขียนรหัสคำสั่งที่สามารถเข้าไปแก้ไขข้อผิดพลาดในโปรแกรมได้ แต่เมื่อเสร็จสิ้นกระบวนการพัฒนาระบบแล้วไม่นำรหัสคำสั่งดังกล่าวออกจากโปรแกรม

____ 2. การทำงานในลักษณะที่ไม่เป็นไปตามลำดับของคำสั่งที่ได้รับโดยขึ้นอยู่กับความพร้อมของอุปกรณ์

____ 3. การปลอมตัวเข้าไปในพื้นที่ที่ไม่ได้รับอนุญาต หรือสวมรอยเป็นผู้มีสิทธิเข้าถึงระบบคอมพิวเตอร์ โดยใช้รหัสลับ ลายนิ้วมือ หรือเสียงของผู้มีสิทธิเข้าถึงที่แท้จริง

____ 4. การลักลอบแก้ไขข้อมูลในระหว่างการับส่งข้อมูลผ่านวงจรสื่อสารรูปแบบต่าง ๆ

____ 5. การจำลองการปฏิบัติงานเพื่อนำผลที่ได้ไปทำทุจริต โดยอาศัยประสิทธิภาพของระบบคอมพิวเตอร์เพื่อวางแผนและสนับสนุนการประกอบอาชญากรรม

____ 6. การซ่อนคำสั่งไว้ในโปรแกรมควบคุมระบบ เมื่อตรงกับวันเดือนปีที่ระบุไว้ โปรแกรมจะสั่งให้คอมพิวเตอร์ทำลายข้อมูลหรือทำให้อุปกรณ์ทำงานผิดพลาด

____ 7. ผู้ทุจริตจะทำการเปลี่ยนแปลงข้อมูล โดยดำเนินการก่อนหรือในระหว่างที่นำข้อมูลเข้าประมวลผล

____ 8. วิธีการยักยอกเงิน สินค้าหรือบริการ จากหลายแหล่ง ทีละเล็กทีละน้อย ทำให้ตรวจจับได้ยาก จนกระทั่งยักยอกไปได้เป็นจำนวนที่สูงมาก

____ 9. การใช้โปรแกรมอรรถประโยชน์ของบริษัทซอฟต์แวร์แห่งหนึ่งในทางที่ไม่ถูกต้อง

____ 10. การซ่อนคำสั่งไม่ประสงค์ดีไว้ในโปรแกรม เพื่อให้โปรแกรมทำตามที่ผู้เขียนโปรแกรมต้องการ

A. Trojan Horse
B. Superzapping
C. Salami Techniques
D. Data Diddling
E. Logic Bombs
F. Trap Doors
G. Asynchronous Attacks
H. Seaverging
I. Data Leakage
J. Piggybacking and Impersonation
K. Wiretapping
L. Simulation and Modeling
M. Ping flood
N. SYN flood
O. IT Governance
P. ระบบตรวจจับการบุกรุก (IDS)
Q. ระบบป้องกันการบุกรุก (IPS)

กิจกรรมที่	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	รวม
คะแนน																