



มาตรฐานอาชีพและคุณวุฒิวิชาชีพ
Occupational Standard and Professional Qualifications

สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย

จัดทำโดย สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)
ร่วมกับ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

1. ชื่อมาตรฐานอาชีพ

สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย

2. ประวัติการปรับปรุงมาตรฐาน

ไม่มี

3. ทะเบียนอ้างอิง (Imprint)

ไม่มี

4. ข้อมูลเบื้องต้น

มาตรฐานสาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network & Security)

มีวัตถุประสงค์สำคัญเพื่อพัฒนาศักยภาพของบุคลากรในสาขาอาชีพ ICT ให้สามารถแข่งขันและเป็นที่ยอมรับในระดับสากล สนับสนุนบุคลากรในกลุ่มอาชีพให้มีสมรรถนะตรงตามความต้องการของผู้ว่าจ้าง มีทักษะทางเทคนิคในการปฏิบัติงาน

5. ประวัติการปรับปรุงมาตรฐานในแต่ละครั้ง

การทบทวนมาตรฐานอาชีพและคุณวุฒิวิชาชีพตามกรอบคุณวุฒิวิชาชีพ 8 ระดับ ครั้งที่ 1

6. ครั้งที่

1 (ปี พุทธศักราช 2563)

การเปลี่ยนแปลงที่สำคัญ

การทบทวนมาตรฐานอาชีพและคุณวุฒิวิชาชีพตามกรอบคุณวุฒิวิชาชีพ 8 ระดับ มีรายละเอียด ดังนี้

- ทบทวนคุณลักษณะผลการเรียนรู้ให้มีความสอดคล้องกับสมรรถนะของคุณวุฒิวิชาชีพ
- ทบทวนการเลื่อนระดับคุณวุฒิวิชาชีพสาขาวิชาชีพ
- ทบทวนสมรรถนะอาชีพ (หน่วยสมรรถนะ หน่วยสมรรถนะย่อย เกณฑ์การปฏิบัติงาน และรายละเอียดหน่วยสมรรถนะ)
- ทบทวนเครื่องมือประเมิน กระบวนการประเมิน คู่มือการประเมิน สัดส่วนคะแนน เกณฑ์การผ่านการประเมิน

กรอบคุณวุฒิ 7 ชั้น จำนวน 5 อาชีพ 16 ชั้นคุณวุฒิ 37 หน่วยสมรรถนะ	กรอบคุณวุฒิ 8 ระดับ จำนวน 5 อาชีพ 16 ระดับคุณวุฒิ 36 หน่วยสมรรถนะ
1. ข่างสนับสนุนด้านเทคนิค ชั้น 3 - 6	1. ข่างสนับสนุนด้านเทคนิค ระดับ 3 - 6
2. นักบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ชั้น 4 - 6	2. นักบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ระดับ 4 - 6
3. นักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ชั้น 4 - 6	3. นักบริหารจัดการความมั่นคงปลอดภัยระบบเครือข่ายและคอมพิวเตอร์ ระดับ 4 - 6
4. นักจัดการความมั่นคงระบบสารสนเทศ ชั้น 4 - 6	4. นักจัดการความมั่นคงระบบสารสนเทศ ระดับ 4 - 6
5. นักจัดการอุปกรณ์พกพาและเครือข่ายไร้สาย ชั้น 4 - 6	5. นักจัดการอุปกรณ์พกพาและเครือข่ายไร้สาย ระดับ 4 - 6

7. คุณวุฒิวิชาชีพที่ครอบคลุม (Professional Qualifications included)

สาขาวิชาชีพอุตสาหกรรมดิจิทัล

สาขาความมั่นคงปลอดภัยทางดิจิทัลและส่วนบุคคล

อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 4

8. คุณวุฒิวิชาชีพที่เกี่ยวข้อง (Related Professional Qualifications)

ไม่มี

9. หน่วยสมรรถนะทั้งหมดในมาตรฐานอาชีพ (List of All Units of Competence within this Occupational Standards)

รหัสหน่วยสมรรถนะ	เนื้อหา
41301	บริหารจัดการระบบและเครือข่าย
41302	วิเคราะห์ความมั่นคงปลอดภัยของระบบและบริหารจัดการข้อมูล
41401	วิเคราะห์การปกป้องเครือข่ายองค์กร ประเมินและจัดการช่องโหว่

10. ระดับคุณวุฒิ

10.1 สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาความมั่นคงปลอดภัยทางดิจิทัลและส่วนบุคคล อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 4

คุณลักษณะของผลการเรียนรู้ (Characteristics of Outcomes)

เป็นผู้มีสมรรถนะทางเทคนิคครอบคลุมในงานจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ที่สามารถแก้ไขปัญหาในบริบทที่คาดการณ์ปัญหาได้ ปรับใช้หลักการหาข้อสรุปประเด็นปัญหาและตัดสินใจงานในหน้าที่ได้ด้วยตนเอง ประสานการทำงานเพื่อควบคุมคุณภาพผลงาน โดยมีสมรรถนะในการบริหารจัดการระบบและเครือข่าย วิเคราะห์ความมั่นคงปลอดภัยของระบบและบริหารจัดการข้อมูล และวิเคราะห์การปกป้องเครือข่ายองค์กร ประเมินและจัดการช่องโหว่

การเลื่อนระดับคุณวุฒิวิชาชีพ (Qualification Pathways)

1. คุณสมบัติของผู้ที่สามารถเข้ารับการประเมินคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 4

- มีประสบการณ์ทำงานด้านจัดการความมั่นคงปลอดภัยระบบสารสนเทศ หรือที่เกี่ยวข้องไม่น้อยกว่า 3 ปี หรือ
- ผู้สำเร็จการศึกษาระดับ ประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) หรือเทียบเท่า ในด้านจัดการความมั่นคงปลอดภัยระบบสารสนเทศ หรือที่เกี่ยวข้อง
- ผู้ที่กำลังศึกษาระดับปริญญาตรี ในด้านจัดการความมั่นคงปลอดภัยระบบสารสนเทศ หรือที่เกี่ยวข้อง

2. ผู้ที่จะผ่านการประเมินและได้รับการรับรองคุณวุฒิวิชาชีพ สาขาวิชาชีพอุตสาหกรรมดิจิทัล สาขาเครือข่ายและความปลอดภัย (Network and Security) อาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 4

- ผ่านเกณฑ์การประเมินตามหน่วยสมรรถนะของอาชีพนักจัดการความมั่นคงปลอดภัยระบบสารสนเทศ ระดับ 4 จำนวน 3 หน่วย

3. ในกรณีต่ออายุหนังสือรับรองมาตรฐานอาชีพให้เป็นไปตามคู่มือสำหรับผู้เข้ารับการประเมินหรือคู่มือเจ้าหน้าที่สอบ

หลักเกณฑ์การต่ออายุหนังสือรับรองมาตรฐานอาชีพ

N/A

กลุ่มบุคคลในอาชีพ (Target Group)

2131.10 นักวิเคราะห์ระบบ

2131.30 ผู้เชี่ยวชาญด้านสื่อสารข้อมูล

2131.60 วิศวกรซอฟต์แวร์

หน่วยสมรรถนะ (หน่วยสมรรถนะทั้งหมดของคุณวุฒิวิชาชีพนี้)

41301 บริหารจัดการระบบและเครือข่าย

41302 วิเคราะห์ความมั่นคงปลอดภัยของระบบและบริหารจัดการข้อมูล

41401 วิเคราะห์การปกป้องเครือข่ายองค์กร ประเมินและจัดการช่องโหว่

ตารางแผนผังแสดงหน้าที่

1. ตารางแสดงหน้าที่ 1

ประกาศใช้ ณ 03/03/2564

ตาราง 1 : FUNCTIONAL MAP แสดง KEY PURPOSE , KEY ROLES , KEY FUNCTION

ความมุ่งหมายหลัก Key Purpose	บทบาทหลัก Key Roles		หน้าที่หลัก Key Function	
	รหัส	คำอธิบาย	รหัส	คำอธิบาย
คำอธิบาย				

คำอธิบาย ตารางแผนผังแสดงหน้าที่เป็นแผนผังที่ใช้วิเคราะห์หน้าที่งานเพื่อให้ได้หน้าที่หลัก (Key Function)

2. ตารางแสดงหน้าที่ 1 (ต่อ)

ประกาศใช้ ณ 03/03/2564

ตาราง 2 : FUNCTIONAL MAP แสดง KEY FUNCTION , UNIT OF COMPETENCE , ELEMENT OF COMPETENCE

หน้าที่หลัก Key Function		หน่วยสมรรถนะ Unit of Competence		หน่วยสมรรถนะย่อย Element of Competence	
รหัส	คำอธิบาย	รหัส	คำอธิบาย	รหัส	คำอธิบาย
413	ปฏิบัติและบำรุงรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	41301	บริหารจัดการระบบและเครือข่าย	41301.01	บริการเครือข่าย
				41301.02	บริหารจัดการระบบ
		41302	วิเคราะห์ความมั่นคงปลอดภัยของระบบและบริหารจัดการข้อมูล	41302.01	วิเคราะห์ความมั่นคงปลอดภัยของระบบ
				41302.02	บริหารจัดการข้อมูล
414	ปกป้องคุ้มครองและสืบสวนทางไซเบอร์	41401	วิเคราะห์การปกป้องเครือข่ายองค์กร ประเมินและจัดการช่องโหว่	41401.01	วิเคราะห์การปกป้องเครือข่ายองค์กร
				41401.02	ประเมินและจัดการช่องโหว่

คำอธิบาย

ตารางแผนผังแสดงหน้าที่ (ต่อ) เป็นแผนผังที่ใช้วิเคราะห์หน้าที่งานหลังจากได้หน้าที่หลัก (Key Function) เพื่อให้ได้ หน่วยสมรรถนะ (Unit of Competence) และหน่วยสมรรถนะย่อย (Element of Competence)

1. รหัสหน่วยสมรรถนะ 41301
2. ชื่อหน่วยสมรรถนะ บริหารจัดการระบบและเครือข่าย
3. ทบทวนครั้งที่ 1 / -
4. สร้างใหม่ ปรับปรุง

5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถบริการและบริหารจัดการระบบเครือข่าย

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. กลุ่มอาชีพ (Sector)

ช่างคอมพิวเตอร์ เจ้าหน้าที่ดูแลระบบเครือข่าย วิศวกรคอมพิวเตอร์ ผู้เชี่ยวชาญระบบเครือข่ายผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบสารสนเทศ

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที

2529 ผู้เชี่ยวชาญด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศและการสื่อสาร

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
41301.01 บริการเครือข่าย	1.1 ออกแบบ ติดตั้งและตั้งค่าอุปกรณ์เครือข่ายตามที่ได้ออกแบบ 1.2 ดำเนินการสำรองข้อมูลบนเครือข่าย 1.3 ติดตามประสิทธิภาพการใช้งานเครือข่าย 1.4 วิเคราะห์แก้ไขปัญหาเครือข่าย แก้ไขปัญหาช่องโหว่ที่เกิดขึ้นภายในเครือข่าย 1.5 ทดสอบและบำรุงรักษาการใช้งานเครือข่ายทั้งฮาร์ดแวร์และซอฟต์แวร์	ข้อสอบข้อเขียน การสัมภาษณ์
41301.02 บริหารจัดการระบบ	2.1 ตรวจสอบและบำรุงรักษาเซิร์ฟเวอร์ให้พร้อมใช้ตามนโยบายขององค์กร 2.2 ออกแบบและตั้งค่านโยบายการเข้าถึงเซิร์ฟเวอร์ จัดการบัญชีรายชื่อผู้ใช้ สิทธิ์ในการเข้าใช้งาน 2.3 ติดตั้งและอัปเดตแพตช์ และ hot fix ต่าง ๆ 2.4 จัดการทรัพยากรภายในระบบ วางแผนการขยายเซิร์ฟเวอร์ให้กับทิศทางขององค์กร	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. สามารถออกแบบ ติดตั้งและตั้งค่าอุปกรณ์เครือข่ายตามที่ได้ออกแบบไว้
2. สามารถดำเนินการสำรองข้อมูลบนเครือข่าย
3. สามารถติดตามประสิทธิภาพการใช้งานเครือข่าย
4. สามารถวิเคราะห์แก้ไขปัญหาเครือข่าย แก้ไขปัญหาช่องโหว่ที่เกิดขึ้นภายในเครือข่าย
5. สามารถทดสอบและบำรุงรักษาการใช้งานเครือข่ายทั้งฮาร์ดแวร์และซอฟต์แวร์
6. สามารถตรวจสอบและบำรุงรักษาเซิร์ฟเวอร์ให้พร้อมใช้ตามนโยบายขององค์กร
7. สามารถออกแบบและตั้งค่านโยบายการเข้าถึงเซิร์ฟเวอร์ จัดการบัญชีรายชื่อผู้ใช้ สิทธิ์ในการใช้งาน
8. สามารถติดตั้งและอัปเดตแพทช์ และ hot fix ต่างๆ
9. สามารถจัดการทรัพยากรภายในระบบ วางแผนการขยายการใช้งานเซิร์ฟเวอร์ให้เหมาะสมกับทิศทางขององค์กร

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับการบริการจัดการเครือข่าย
2. ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยของเครือข่าย
3. ความรู้เกี่ยวกับเทคโนโลยีการรักษาความมั่นคงปลอดภัยของเครือข่าย
4. ความรู้เกี่ยวกับการออกแบบเครือข่ายที่มีความมั่นคงปลอดภัย
5. ความรู้เกี่ยวกับการบริการจัดการระบบ
6. ความรู้เกี่ยวกับระบบปฏิบัติการ
7. ความรู้เกี่ยวกับ Cloud และ Virtualization

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมินและควรที่จะใช้ประกอบร่วมกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการสัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ได้รับประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ในการปฏิบัติงานให้คำนึงถึงการบริการเครือข่าย การบริหารจัดการระบบ

(ข) คำอธิบายรายละเอียด

1. การบริการเครือข่าย การออกแบบ ติดตั้งและตั้งค่าอุปกรณ์เครือข่ายตามที่ได้ออกแบบไว้ ให้ทำการวิเคราะห์ความต้องการของผู้ใช้และข้อจำกัด ความต้องการของระบบ คุณสมบัติที่ต้องการ สภาพแวดล้อมของเครือข่ายที่เป็นอยู่ เพื่อนำไปใช้ในการออกแบบที่เหมาะสม การดำเนินการสำรองข้อมูลบนเครือข่าย ให้พิจารณาความต้องการของเครือข่ายเป็นหลักในการเลือกแนวทางการสำรองข้อมูล เช่น ความพร้อมใช้ ระยะเวลาที่ยอมให้ข้อมูลสูญหายได้ เป็นต้น การติดตามประสิทธิภาพการใช้งานเครือข่าย ให้เลือกเครื่องมือที่เหมาะสม คัดเลือกบุคลากรที่มีความสามารถ การวิเคราะห์แก้ไขปัญหาเครือข่าย แก้ไขปัญหาช่องโหว่ที่เกิดขึ้นภายในเครือข่าย ให้เน้นในด้านกระบวนการจัดการแก้ไขปัญหา โดยอ้างอิงกับข้อกำหนดต่าง ๆ ที่อาจมี เช่น Service Level Agreement (SLA)

เป็นต้น การทดสอบและบำรุงรักษาการใช้งานเครือข่ายทั้งฮาร์ดแวร์และซอฟต์แวร์ ให้มีการดำเนินการอย่างสม่ำเสมอและพิจารณาปรับเปลี่ยนอุปกรณ์ทดแทนตามวงรอบ

2. การบริหารจัดการระบบ การตรวจสอบและบำรุงรักษาเซิร์ฟเวอร์ให้พร้อมใช้ตามนโยบายขององค์กร ให้มีการวางแผนการตรวจสอบเป็นระยะ อาจมีการสร้างฟอร์มและ checklist สำหรับการตรวจสอบ การออกแบบและตั้งค่านโยบายการเข้าถึงเซิร์ฟเวอร์ จัดการบัญชีรายชื่อผู้ใช้ สิทธิในการเข้าใช้งาน ให้อ้างอิงตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรเป็นหลัก การติดตั้งและอัปเดตแพทช์ และ hot fix ต่าง ๆ ให้ทำรายการแหล่งข้อมูลอ้างอิงจากผู้ผลิต การอัปเดตแพทช์ รวมทั้งมีการสร้างกระบวนการ patch management และ change management การจัดการทรัพยากรภายในระบบ วางแผนการขยายการใช้งานเซิร์ฟเวอร์ให้เหมาะสมกับทิศทางขององค์กร ให้พิจารณาจากความต้องการทางด้านระบบขององค์กร

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 41301.01 บริการเครือข่าย ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 41301.02 บริหารจัดการระบบ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

1. รหัสหน่วยสมรรถนะ 41302
2. ชื่อหน่วยสมรรถนะ วิเคราะห์ความมั่นคงปลอดภัยของระบบและบริหารจัดการข้อมูล
3. ทบทวนครั้งที่ 1 / -
4. สร้างใหม่ ปรับปรุง
5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถ วิเคราะห์ความมั่นคงปลอดภัยของระบบ บริหารจัดการข้อมูล ที่มีความมั่นคงปลอดภัย

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. กลุ่มอาชีพ (Sector)

ช่างคอมพิวเตอร์ เจ้าหน้าที่ดูแลระบบเครือข่าย วิศวกรคอมพิวเตอร์ ผู้เชี่ยวชาญระบบเครือข่าย ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบสารสนเทศ

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที

2529 ผู้เชี่ยวชาญด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศและการสื่อสาร

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
41302.01 วิเคราะห์ความมั่นคงปลอดภัยของระบบ	1.1 ตรวจสอบเพื่อให้มั่นใจว่าได้มีการอุดช่องโหว่ของแอปพลิเคชันทั้งหมดภายในระบบ 1.2 กำหนดการควบคุมการเข้าถึงตามแนวทางของ least privilege และ need to know 1.3 ทบทวนความมั่นคงปลอดภัยของระบบเพื่อให้แน่ใจว่าความเสี่ยงต่าง ๆ ได้รับการจัดการ	ข้อสอบข้อเขียน การสัมภาษณ์
41302.02 บริหารจัดการข้อมูล	2.1 วิเคราะห์ความต้องการ ออกแบบ วางแผน การจัดการข้อมูล 2.2 ออกแบบ ติดตั้ง และบำรุงรักษาระบบฐานข้อมูล data mining และ data warehouse 2.3 ดำเนินการสำรองและกู้คืนข้อมูล	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. สามารถตรวจสอบเพื่อให้มั่นใจว่าได้มีการอุดช่องโหว่ของแอปพลิเคชันทั้งหมดภายในระบบ
2. สามารถกำหนดการควบคุมการเข้าถึงตามแนวทางของ least privilege และ need to know
3. สามารถทบทวนความมั่นคงปลอดภัยของระบบเพื่อให้มั่นใจว่าความเสี่ยงต่าง ๆ ได้รับการจัดการอย่างเหมาะสม
4. สามารถวิเคราะห์ความต้องการ ออกแบบ วางแผน การจัดการข้อมูล
5. สามารถออกแบบ ติดตั้ง และบำรุงรักษาฐานข้อมูล data mining และ data warehouse ให้มีประสิทธิภาพที่เหมาะสม
6. สามารถดำเนินการสำรองและกู้คืนข้อมูล

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับระบบสารสนเทศและระบบเครือข่าย
2. ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ
3. ความรู้เกี่ยวกับการออกแบบระบบสารสนเทศที่มีความมั่นคงปลอดภัย
4. ความรู้เกี่ยวกับการพัฒนาระบบฐานข้อมูล
5. ความรู้เกี่ยวกับการจัดการข้อมูล

14. หลักฐานที่ต้อการ (Evidence Guide)

หลักฐานที่ต้อการจะกำหนดข้อแนะนำเกี่ยวกับการประเมิน และควรที่จะใช้ประกอบร่วมกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้อการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการสัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ได้รับประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ในการปฏิบัติงานให้คำนึงถึงการวิเคราะห์ความมั่นคงปลอดภัยของระบบและการบริหารจัดการข้อมูล

(ข) คำอธิบายรายละเอียด

1. การวิเคราะห์ความมั่นคงปลอดภัยของระบบ การตรวจสอบเพื่อให้มั่นใจว่าได้มีการอุดช่องโหว่ของแอปพลิเคชันทั้งหมดภายในระบบ อาจทำได้หลายวิธีทั้งแบบ Static code analysis และ Dynamic analysis การกำหนดการควบคุมการเข้าถึงตามแนวทางของ least privilege และ need to know อาจดำเนินการทั้งในระดับของแอปพลิเคชันและระดับระบบปฏิบัติการ การทบทวนความมั่นคงปลอดภัยของระบบเพื่อให้มั่นใจว่าความเสี่ยงต่าง ๆ ได้รับการจัดการอย่างเหมาะสม ให้มีการดำเนินการอย่างสม่ำเสมอ และมีการบันทึกผลการทบทวนทุกครั้ง

2. การบริหารจัดการข้อมูล การวิเคราะห์ความต้องการ ออกแบบ วางแผน การจัดการข้อมูล ทำการวิเคราะห์และกำหนดความต้องการด้านข้อมูล วิเคราะห์และวางแผนการปรับเปลี่ยนความต้องการด้านข้อมูล การออกแบบ ติดตั้ง และบำรุงรักษาฐานข้อมูล data mining และ data warehouse ให้มีประสิทธิภาพที่เหมาะสม ทบทวนและตรวจสอบระบบ data mining และ data warehouse พัฒนามาตรฐาน นโยบาย และขั้นตอนปฏิบัติงานด้านการจัดการข้อมูลบำรุงรักษาและแก้ไขปัญหาทางด้านระบบฐานข้อมูล การดำเนินการสำรองและกู้คืนข้อมูล ให้พิจารณาระดับความพร้อมใช้ของข้อมูล และระยะเวลาที่ยอมให้ข้อมูลสูญหายได้ และมีการวางแผนและทำการทดสอบการกู้คืนข้อมูลเป็นระยะอย่างสม่ำเสมอ

16. หน่วยสมรรถนะรวม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 41302.01 วิเคราะห์ความมั่นคงปลอดภัยของระบบ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 41302.02 บริหารจัดการข้อมูล ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์

1. รหัสหน่วยสมรรถนะ 41401
2. ชื่อหน่วยสมรรถนะ วิเคราะห์การปกป้องเครือข่ายองค์กร ประเมินและจัดการช่องโหว่
3. ทบทวนครั้งที่ 1 / -
4. สร้างใหม่ ปรับปรุง
5. สำหรับชื่ออาชีพและรหัสอาชีพ (Occupational Classification)

6. คำอธิบายหน่วยสมรรถนะ (Description of Unit of Competency)

เป็นผู้ที่สามารถ วิเคราะห์การปกป้องเครือข่ายองค์กร ประเมินและจัดการช่องโหว่ ที่มีความมั่นคงปลอดภัย

7. สำหรับระดับคุณวุฒิ

1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. กลุ่มอาชีพ (Sector)

เป็นช่างคอมพิวเตอร์ เจ้าหน้าที่ดูแลระบบเครือข่าย วิศวกรคอมพิวเตอร์ ผู้เชี่ยวชาญระบบเครือข่ายผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบสารสนเทศ

9. ชื่ออาชีพและรหัสอาชีพอื่นที่หน่วยสมรรถนะนี้สามารถใช้ได้ (ถ้ามี)

2131.50 ผู้เชี่ยวชาญด้านความปลอดภัยของไอที

2529 ผู้เชี่ยวชาญด้านความปลอดภัยในระบบเทคโนโลยีสารสนเทศและการสื่อสาร

10. ข้อกำหนดหรือกฎระเบียบที่เกี่ยวข้อง (Licensing or Regulation Related) (ถ้ามี)

ไม่มี

11. สมรรถนะย่อยและเกณฑ์การปฏิบัติงาน (Elements and Performance Criteria)

สมรรถนะย่อย (Element)	เกณฑ์ในการปฏิบัติงาน (Performance Criteria)	วิธีการประเมิน (Assessment)
41401.01 วิเคราะห์การปกป้องเครือข่ายองค์กร	1.1 วิเคราะห์ข้อมูลภายในเครือข่ายเพื่อตรวจหากิจกรรมผิดปกติ ช่องโหว่และภัยคุกคามต่อองค์กร 1.2 ดำเนินงาน Defense-in-depth เพื่อการรักษาความมั่นคงปลอดภัยของเครือข่ายองค์กร	ข้อสอบข้อเขียน การสัมภาษณ์
41401.02 ประเมินและจัดการช่องโหว่	2.1 ดำเนินการตรวจสอบช่องโหว่ และการเจาะระบบ 2.2 จัดทำรายงานผลการตรวจสอบช่องโหว่และการเจาะระบบ 2.3 ให้คำแนะนำในการเลือกเทคนิคและเทคโนโลยีที่เหมาะสมเพื่อบรรเทาความเสี่ยงทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ	ข้อสอบข้อเขียน การสัมภาษณ์

12. ความรู้และทักษะก่อนหน้าที่จำเป็น (Pre-requisite Skill & Knowledge)

ไม่มี

13. ทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) ความต้องการด้านทักษะ

1. สามารถวิเคราะห์ข้อมูลภายในเครือข่ายเพื่อตรวจหากิจกรรมผิดปกติ ช่องโหว่และภัยคุกคามต่อองค์กร
2. สามารถดำเนินงาน Defense-in-depth เพื่อการรักษาความมั่นคงปลอดภัยของเครือข่ายองค์กร
3. สามารถดำเนินการตรวจสอบช่องโหว่ และการเจาะระบบ
4. สามารถจัดทำรายงานผลการตรวจสอบช่องโหว่และการเจาะระบบ
5. สามารถให้คำแนะนำในการเลือกเทคนิคและเทคโนโลยีที่เหมาะสมเพื่อบรรเทาความเสี่ยงทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ

(ข) ความต้องการด้านความรู้

1. ความรู้เกี่ยวกับวิทยาการเข้ารหัสลับ
2. ความรู้เกี่ยวกับการสำรองข้อมูล
3. ความรู้เกี่ยวกับระบบปฏิบัติการและระบบเครือข่าย
4. ความรู้เกี่ยวกับอุปกรณ์ทางด้านความมั่นคงปลอดภัย เช่น ระบบตรวจจับการบุกรุก ไฟร์วอลล์
5. ความรู้เกี่ยวกับการตอบสนองต่อภัยคุกคามทางไซเบอร์
6. ความรู้เกี่ยวกับช่องโหว่และภัยคุกคามของระบบและเครือข่าย
7. ความรู้เกี่ยวกับเครื่องมือวิเคราะห์ช่องโหว่
8. ความรู้เกี่ยวกับการโจมตีประเภทต่าง ๆ
9. ความรู้เกี่ยวกับระบบปฏิบัติการและระบบเครือข่าย
10. ความรู้เกี่ยวกับขั้นตอนในการโจมตีระบบและเครือข่าย

14. หลักฐานที่ต้องการ (Evidence Guide)

หลักฐานที่ต้องการจะกำหนดข้อแนะนำเกี่ยวกับการประเมิน และควรที่จะใช้ประกอบร่วมกับเกณฑ์การปฏิบัติงาน (Performance Criteria) และทักษะและความรู้ที่ต้องการ (Required Skills and Knowledge)

(ก) หลักฐานการปฏิบัติงาน (Performance Evidence)

1. เอกสารหลักฐานที่จำเป็นในการปฏิบัติงาน

(ข) หลักฐานความรู้ (Knowledge Evidence)

1. ผลการทดสอบความรู้
2. ผลการสัมภาษณ์

(ค) คำแนะนำในการประเมิน

ผู้เข้ารับการประเมินต้องผ่านการประเมิน ที่ครอบคลุมในทุกสมรรถนะประเมินย่อย ขอบเขต ความรู้และทักษะที่กำหนด ในกรณีที่ได้รับประเมินผ่านไม่ครบตามเกณฑ์ที่กำหนด ผู้ประเมินจะต้องแจ้งหน่วยสมรรถนะที่ไม่ผ่าน และให้ผู้รับการประเมินไปทบทวนสมรรถนะที่ยังไม่ผ่านและสามารถกลับมาทดสอบสมรรถนะใหม่อีกครั้ง

(ง) วิธีการประเมิน

1. ทดสอบโดยใช้แบบข้อเขียน
2. ทดสอบโดยใช้แบบสัมภาษณ์

15. ขอบเขต (Range Statement)

(ก) คำแนะนำ

ในการปฏิบัติงานให้คำนึงถึงการวิเคราะห์การปกป้องเครือข่ายองค์กรการประเมินและจัดการช่องโหว่

(ข) คำอธิบายรายละเอียด

1. การวิเคราะห์การปกป้องเครือข่ายองค์กร การวิเคราะห์ข้อมูลภายในเครือข่ายเพื่อตรวจหากิจกรรมผิดปกติ ช่องโหว่และภัยคุกคามต่อองค์กร ดำเนินการวางแผนการวิเคราะห์ความมั่นคงปลอดภัยของระบบและเครือข่าย จัดหาเครื่องมือในการสนับสนุนการวิเคราะห์ความมั่นคงปลอดภัยของระบบและเครือข่าย ทำการวิเคราะห์ข้อมูลที่ได้รับจากระบบและเครือข่ายผ่านทางอุปกรณ์และเครื่องมือต่าง ๆ เพื่อระบุภัยคุกคามที่มีต่อองค์กร จัดทำรายงานสรุปผลของการวิเคราะห์ความมั่นคงปลอดภัยของระบบและเครือข่าย การดำเนินงาน Defense-in-depth เพื่อการรักษาความมั่นคงปลอดภัยของเครือข่ายองค์กร ให้พิจารณาดำเนินการให้สอดคล้องกับนโยบายและแนวปฏิบัติทางการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร
2. การประเมินและจัดการช่องโหว่ การดำเนินการตรวจสอบช่องโหว่ และการเจาะระบบ ควรมีการวิเคราะห์ขอบเขตที่เหมาะสมของก่อนดำเนินการ โดยอาจทำการตรวจสอบช่องโหว่ก่อนเพื่อทราบข้อมูลเบื้องต้นว่าระบบสารสนเทศและเครือข่ายมีโอกาสถูกเจาะจากช่องทางใดบ้าง

จากนั้นจึงดำเนินการพิจารณาทำการเจาะระบบ โดยที่มีสิ่งที่จะต้องพิจารณาคือการเจาะระบบมีโอกาสที่จะทำให้การดำเนินการของระบบหยุดชะงัก ดังนั้นหากพิจารณาที่จะทำการเจาะระบบ ควรมีเจ้าหน้าที่ผู้ดูแลระบบทำการเตรียมพร้อมในการนำระบบขึ้นหากเกิดระบบล่มในช่วงเวลาที่มีการดำเนินการ จัดทำรายงานผลการตรวจสอบช่องโหว่และการเจาะระบบ ให้นำไปทบทวนเป้าหมายของการทดสอบ และให้ใช้ภาษาที่เข้าใจง่าย การให้คำแนะนำในการเลือกเทคนิคและเทคโนโลยีที่เหมาะสมเพื่อบรรเทาความเสี่ยงทางด้านความมั่นคงปลอดภัยระบบสารสนเทศ โดยอ้างอิงจากผลที่ได้รับจากการทดสอบ

16. หน่วยสมรรถนะร่วม (ถ้ามี)

ไม่มี

17. อุตสาหกรรมร่วม/กลุ่มอาชีพร่วม (ถ้ามี)

ไม่มี

18. รายละเอียดกระบวนการและวิธีการประเมิน (Assessment Description and Procedure)

วิธีการประเมินสามารถจำแนกได้ตามสมรรถนะย่อย ดังนี้

1. สมรรถนะย่อย 41401.01 วิเคราะห์การปกป้องเครือข่ายองค์กร ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์
2. สมรรถนะย่อย 41401.02 ประเมินและจัดการช่องโหว่ ให้ทำการทดสอบโดยใช้แบบข้อเขียนและทดสอบโดยใช้แบบสัมภาษณ์