บทที่ 4

ผลการวิจัยและวิเคราะห์ข้อมูล

4.1 ผลการวิเคราะห์เชิงพรรณนา

ผลจากการตอบแบบสอบถามภายในองค์กรกรณีตัวอย่างโดยเก็บข้อมูลจากทั้งองค์กรที่มีพนักงานประจำจำนวนประมาณ 160 คน แต่ได้แบบสอบถามกลับมาจำนวน 110 คน เนื่องจากผู้ที่ไม่สามารถตอบแบบสอบถามได้นั้น ส่วนหนึ่งเป็นผู้บริหารระดับสูงและอีกส่วนเป็นพนักงานที่ประจำตามต่างจังหวัด

4.1.1 ลักษณะประชากรของกลุ่มตัวอย่าง

เป็นข้อมูลทั่วไปของผู้ตอบแบบสอบถามทั้งหมด 110 คน ซึ่งสามารถจำแนกได้ดังนี้

- คิดเป็นเพศชาย 52.73% และเพศหญิง 47.27% ดังแสดงในตารางที่ 4.1 และภาพที่ 4.1
- อยู่ในช่วงอายุ21-25 ปี 43.63%, อายุ26-30 ปี 40.91%, อายุ31-35 ปี 12.73% และอายุ 35-40 ปี 2.73% ดังแสดงในตารางที่ 4.2 และภาพที่ 4.2
- การศึกษาระดับปริญญาตรี 70% และ ปริญญาโท 30% ดังแสดงในตารางที่ 4.3 และภาพที่ 4.3
- ระยะเวลาของประสบการณ์ทำงาน ช่วงน้อยกว่า1 ปี 11.82%, 1 - 2 ปี 28.18%, 3 - 4 ปี 30%และช่วงประสบการณ์ทำงานระหว่าง 5 - 10 ปี 5.45% ดังแสดงในตารางที่ 4.4 และภาพที่ 4.4
- ระยะเวลาการทำงานในองค์กรปัจจุบัน น้อยกว่า 1 ปี 17.27%, 1 - 2 ปี 42.73%, 3 - 4 ปี 22.73%, มากกว่า 4 ปี 17.27% ดังแสดงในตารางที่ 4.5 และภาพที่ 4.5
- แบ่งตามตำแหน่งงานเป็น ฝ่ายปฏิบัติการ 90.91% และ ฝ่ายบริหาร 9.09% ดังแสดงในตารางที่ 4.6 และภาพที่ 4.6
- โดยพบว่าเป็นพนักงานด้าน IT 40%และ Non-IT 60% ดังแสดงในตารางที่ 4.7 และภาพที่ 4.7

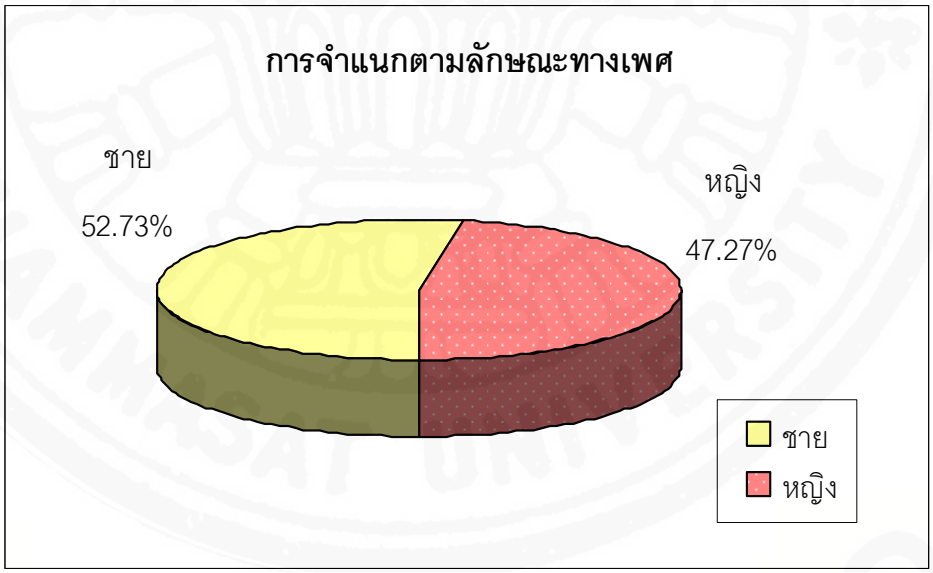
ตารางที่ 4.1

จำนวนเปอร์เซ็นต์ ของกลุ่มตัวอย่างทั้งหมด จำแนกตามลักษณะเพศ

เพศ	กลุ่มตัวอย่าง	
	จำนวน	%
ชาย	58	52.73
หญิง	52	47.27
รวม	**110**	**100**

ภาพที่ 4.1

กราฟเปอร์เซ็นต์ ของกลุ่มตัวอย่างทั้งหมด จำแนกตามลักษณะเพศ



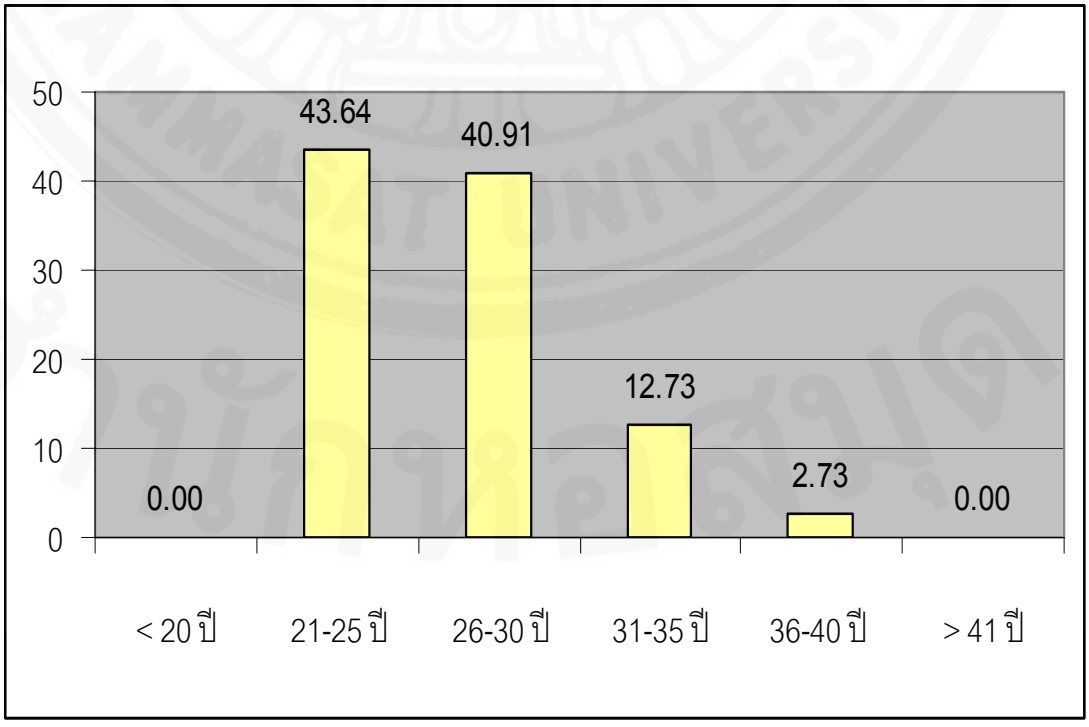
ตารางที่ 4.2

จำนวนเปอร์เซ็นต์ ของกลุ่มตัวอย่างทั้งหมด จำแนกตามช่วงอายุของผู้ตอบแบบสอบถาม

ช่วงอายุ	กลุ่มตัวอย่าง	
	จำนวน	%
ต่ำกว่า 20 ปี	0	0
21-25 ปี	48	43.63
26-30 ปี	45	40.91
31-35 ปี	14	12.73
36-40 ปี	3	2.73
มากกว่า 40 ปี	0	0
รวม	**110**	**100**

ภาพที่ 4.2

กราฟเปอร์เซ็นต์ ของกลุ่มตัวอย่างทั้งหมด จำแนกตามช่วงอายุของผู้ตอบแบบสอบถาม



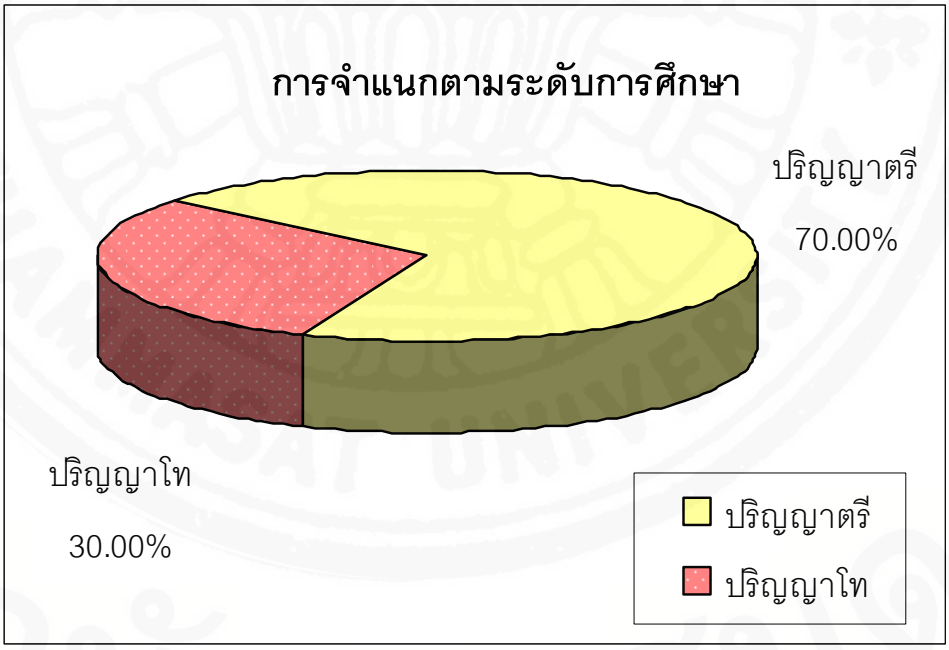
ตารางที่ 4.3

จำนวนเปอร์เซ็นต์ ของกลุ่มตัวอย่างทั้งหมด จำแนกตามระดับการศึกษา

ระดับการศึกษา	กลุ่มตัวอย่าง	
	จำนวน	%
ปริญญาตรี	77	70
ปริญญาโท	33	30
รวม	**110**	**100**

ภาพที่ 4.3

กราฟเปอร์เซ็นต์ ของกลุ่มตัวอย่างทั้งหมด จำแนกตามระดับการศึกษา



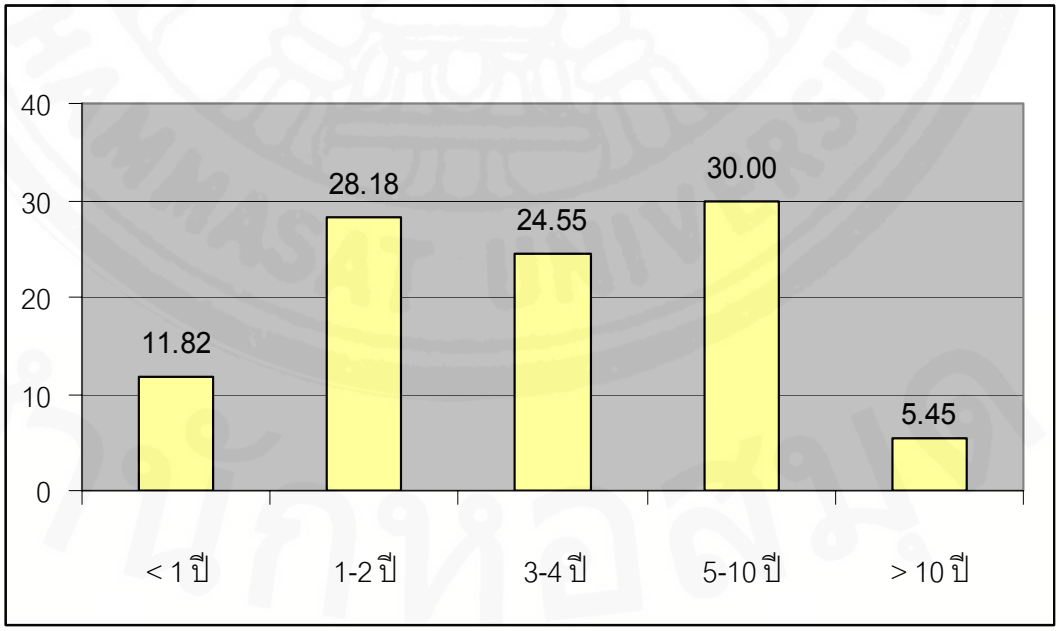
ตารางที่ 4.4

จำนวนเปอร์เซ็นต์ ของกลุ่มตัวอย่างทั้งหมด จำแนกตามประสบการณ์ทำงาน

ประสบการณ์ทำงาน	กลุ่มตัวอย่าง	
	จำนวน	จำนวน
น้อยกว่า 1 ปี	13	11.82
1 - 2 ปี	31	28.18
3 - 4 ปี	27	24.55
5 - 10 ปี	33	30.00
มากกว่า 10 ปี	6	5.45
รวม	**110**	**100**

ภาพที่ 4.4

กราฟเปอร์เซ็นต์ของกลุ่มตัวอย่างทั้งหมด จำแนกตามประสบการณ์ทำงาน



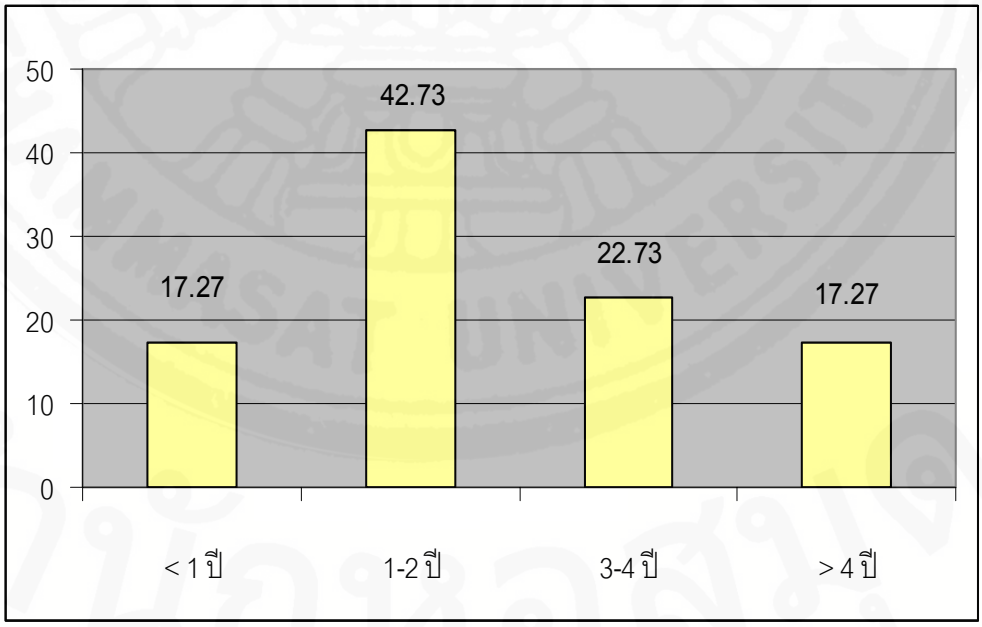
ตารางที่ 4.5

จำนวนเปอร์เซ็นต์ของกลุ่มตัวอย่างทั้งหมด จำแนกตามระยะเวลาการทำงานในองค์กรปัจจุบัน

ระยะเวลาการทำงานในองค์กรปัจจุบัน	กลุ่มตัวอย่าง	
	จำนวน	%
น้อยกว่า 1 ปี	19	17.27
1 - 2 ปี	47	42.73
3 - 4 ปี	25	22.73
มากกว่า 4 ปี	19	17.27
รวม	**110**	**100**

ภาพที่ 4.5

กราฟเปอร์เซ็นต์ของกลุ่มตัวอย่างทั้งหมด จำแนกตามระยะเวลาการทำงานในองค์กรปัจจุบัน



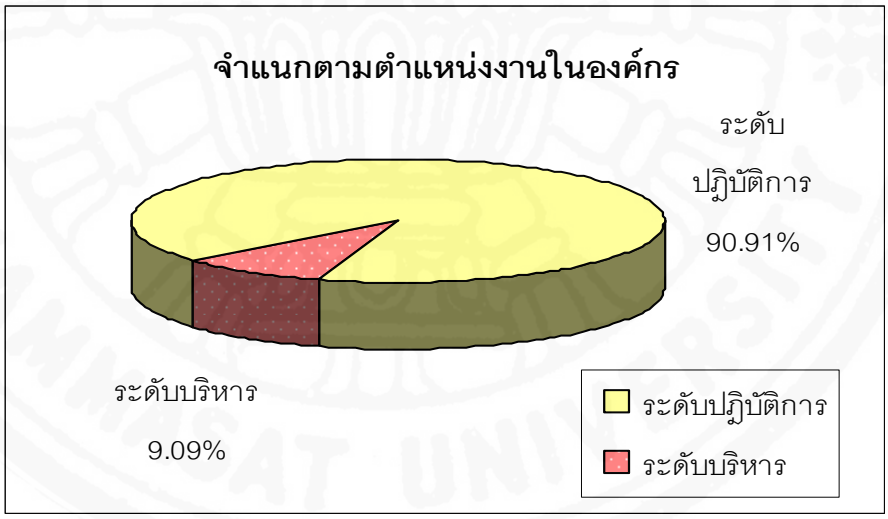
ตารางที่ 4.6

จำนวนเปอร์เซ็นต์ของกลุ่มตัวอย่างทั้งหมด จำแนกตามตำแหน่งงานในองค์กร

ตำแหน่งงานในองค์กร	กลุ่มตัวอย่าง	
	จำนวน	%
ระดับปฏิบัติการ	100	90.91
ระดับบริหาร	10	9.09
รวม	**110**	**100**

ภาพที่ 4.6

กราฟเปอร์เซ็นต์ของกลุ่มตัวอย่างทั้งหมด จำแนกตามตำแหน่งงานในองค์กร



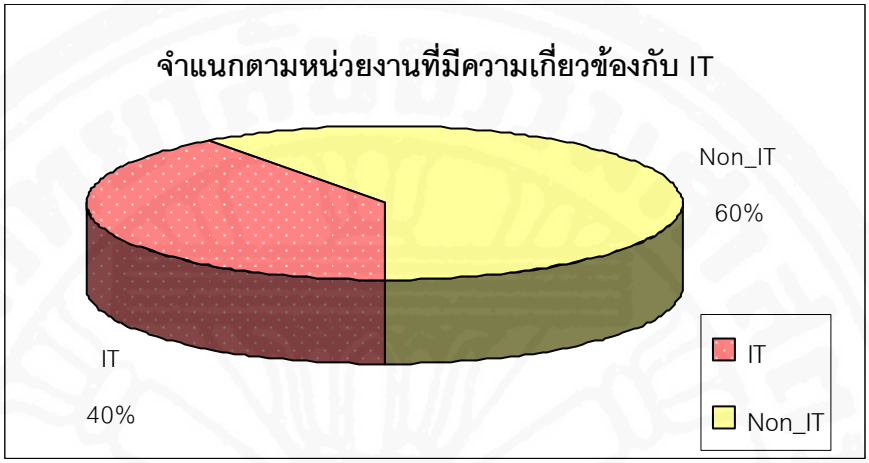
ตารางที่ 4.7

จำนวนเปอร์เซ็นต์ของกลุ่มตัวอย่างทั้งหมด จำแนกตามหน่วยงานที่สังกัดในองค์กร

หน่วยงานที่สังกัดในองค์กร	กลุ่มตัวอย่าง	
	จำนวน	%
หน่วยงานที่เกี่ยวข้องกับ IT(IT)	44	40
หน่วยงานที่ไม่เกี่ยวข้องกับ IT(Non-IT)	66	60
รวม	**110**	**100**

ภาพที่ 4.7

กราฟเปอร์เซ็นต์ของกลุ่มตัวอย่างทั้งหมด จำแนกตามหน่วยงานที่สังกัดในองค์กร



4.1.2 ผลสำรวจความคิดเห็น ด้านการรักษาความปลอดภัยระบบสารสนเทศในองค์กรตามมาตรฐาน ISO17799

การจัดการเพื่อรักษาความปลอดภัยของข้อมูลตามมาตรฐาน ISO 17799 นั้นมีทั้งหมด 11 หัวข้อ โดยข้อมูลที่ได้จากแบบสอบถามมานั้นเป็นการแสดงความคิดเห็นของพนักงานในองค์กรต่อมาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศของตัวองค์กรที่อิงตามมาตรฐาน ISO17799 โดยสามารถสรุปตามหัวข้อของมาตรฐานดังกล่าวได้ ดังนี้

4.1.2.1 ผลสำรวจด้าน นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

ตารางที่ 4.8

ผลสำรวจความคิดเห็นด้านการรับรู้นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศในองค์กร

ผลสำรวจ	ไม่ทราบ	ทราบ
ท่านทราบหรือไม่ว่าปัจจุบันองค์กรมีการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร (1= ไม่ทราบ , 5 = ทราบ)	35	75

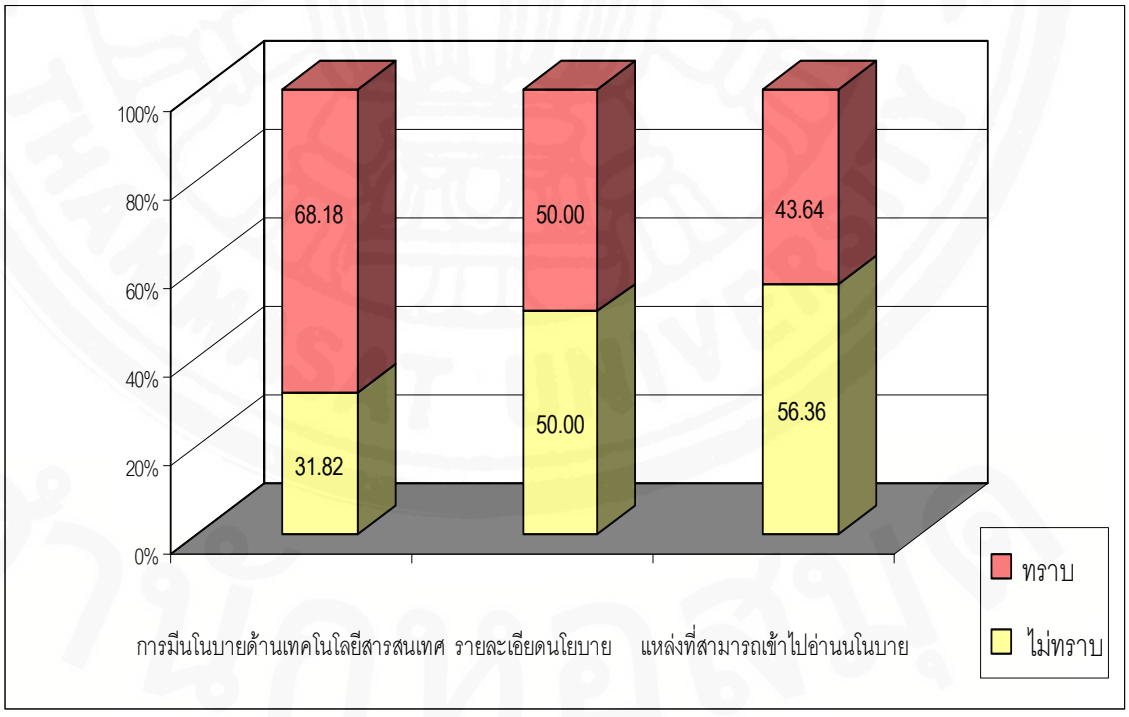
ตารางที่ 4.8 (ต่อ)

ผลสำรวจความคิดเห็นด้านการรับรู้นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศในองค์กร

ผลสำรวจ	ไม่ทราบ	ทราบ
ท่านทราบรายละเอียดของนโยบายดังกล่าวหรือไม่ (1= ไม่ทราบ , 5 = ทราบ)	55	55
ท่านทราบแหล่งที่สามารถเข้าไปอ่านนโยบายดังกล่าวหรือไม่ (1= ไม่ทราบ , 5= ทราบ)	62	48
รวม	152	178
% เฉลี่ยรวม	46.06	53.93

ภาพที่ 4.8

กราฟเปอร์เซ็นต์ของกลุ่มตัวอย่างทั้งหมด จากผลสำรวจด้านการรับรู้นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศในองค์กร



4.1.2.2 ผลสำรวจด้าน โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)

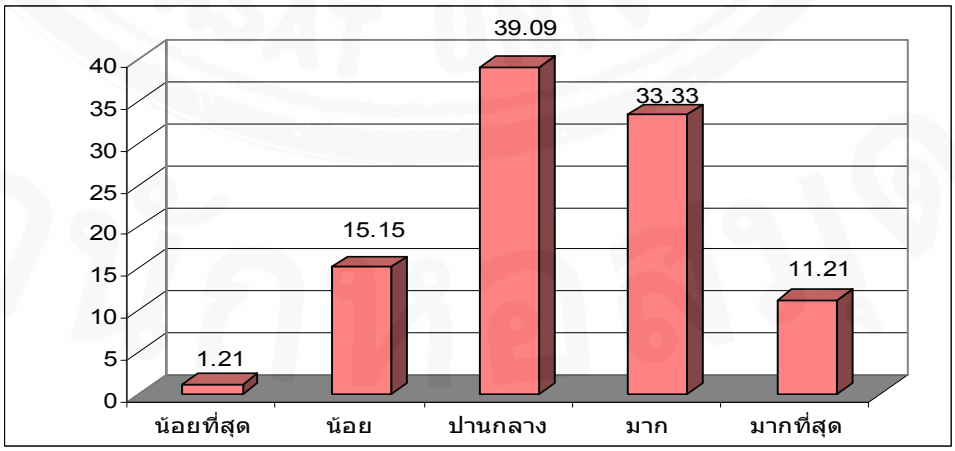
ตารางที่ 4.9

ผลสำรวจความคิดเห็นด้านโครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร และที่เกี่ยวกับลูกค้าหรือหน่วยงานภายนอก

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านทราบหน้าที่ความผิดชอบของท่านในการรักษาความปลอดภัยด้านระบบสารสนเทศมากน้อยเพียงใด	2	27	43	33	5
ท่านทราบเรื่องการรักษาและไม่เปิดเผยความลับขององค์กรมากน้อยเพียงใด	2	13	37	38	20
ท่านเห็นว่ามาตรฐานขององค์กรในการให้บริการธุรกรรมออนไลน์ ปัจจุบันมีความปลอดภัยด้านข้อมูลมากน้อยเพียงใด	0	10	49	39	12
รวม	**4**	**50**	**129**	**110**	**37**
% เฉลี่ยรวม	**1.21**	**15.15**	**39.09**	**33.33**	**11.21**

ภาพที่ 4.9

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้านด้านโครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก



4.1.2.3 ผลสำรวจด้าน หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)

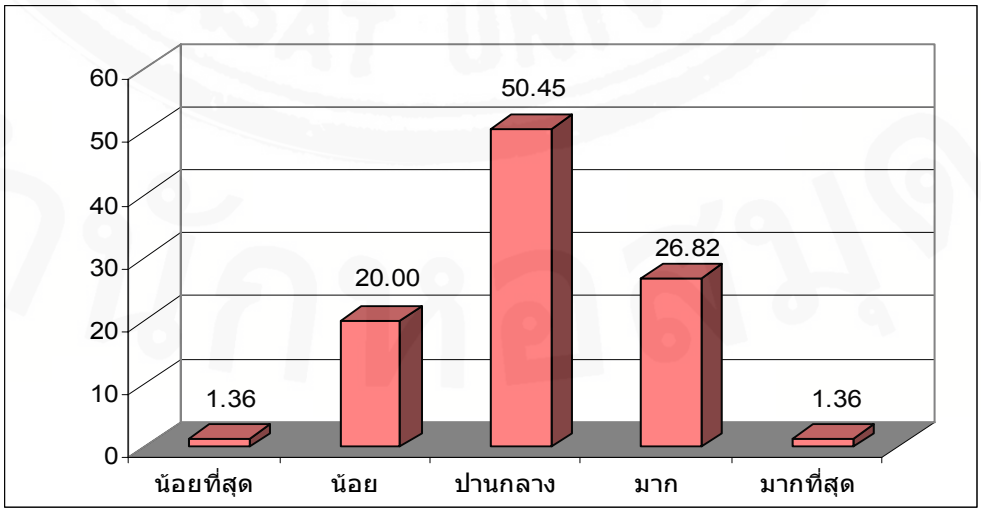
ตารางที่ 4.10

ผลสำรวจความคิดเห็นด้านหน้าที่ความรับผิดชอบต่อทรัพย์สินและการจัดหมวดหมู่สารสนเทศ

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศมากน้อยแค่ไหน	1	28	54	26	1
ท่านสามารถแบ่งประเภทของข้อมูลได้มากน้อยแค่ไหน เช่น ข้อมูลลับ(Secret Information),ข้อมูลลับเฉพาะ(Confidential Information),ข้อมูลที่จำเป็นมาก(Critical Information),ข้อมูลสาธารณะหรือข้อมูลทั่วไป	2	16	57	33	2
รวม	3	44	111	59	3
% เฉลี่ยรวม	1.36	20	50.45	26.82	1.36

ภาพที่ 4.10

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้านหน้าที่ความรับผิดชอบต่อทรัพย์สินและการจัดหมวดหมู่สารสนเทศ



4.1.2.4 ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)

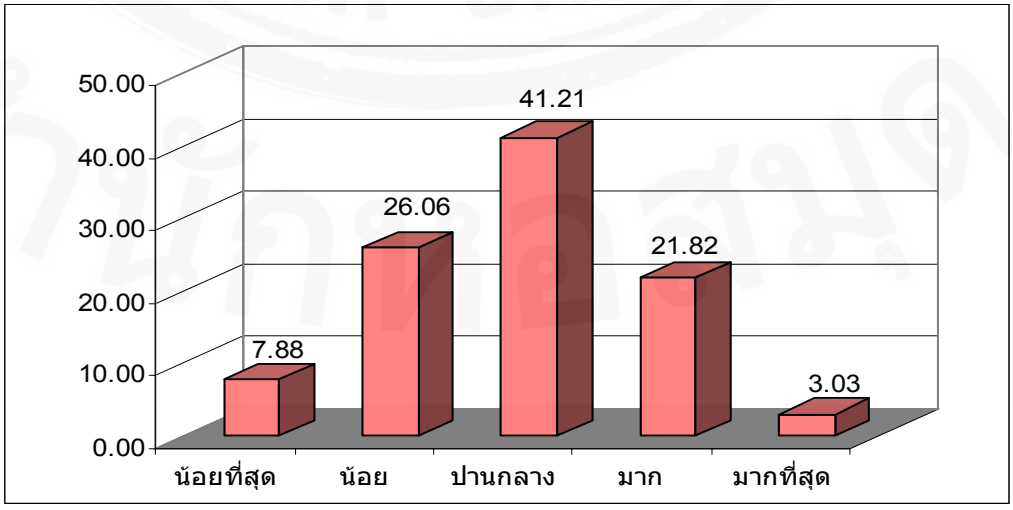
ตารางที่ 4.11

ผลสำรวจความคิดเห็นด้านความมั่นคงปลอดภัยของระบบสารสนเทศก่อนและระหว่างการจ้างงาน

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านคิดว่าการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์(Application) ต่างๆภายในองค์กรมีความเหมาะสมเพียงใดในปัจจุบัน	1	4	49	49	7
ท่านเคยได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศมากน้อยแค่ไหน	12	39	44	14	1
ท่านทราบบทลงโทษสำหรับพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กรมากน้อยแค่ไหน	13	43	43	9	2
รวม	26	86	136	72	10
% เฉลี่ยรวม	7.88	26.06	41.21	21.82	3.03

ภาพที่ 4.11

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้านการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศทั้งก่อนและระหว่างการจ้างงาน



4.1.2.5 ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

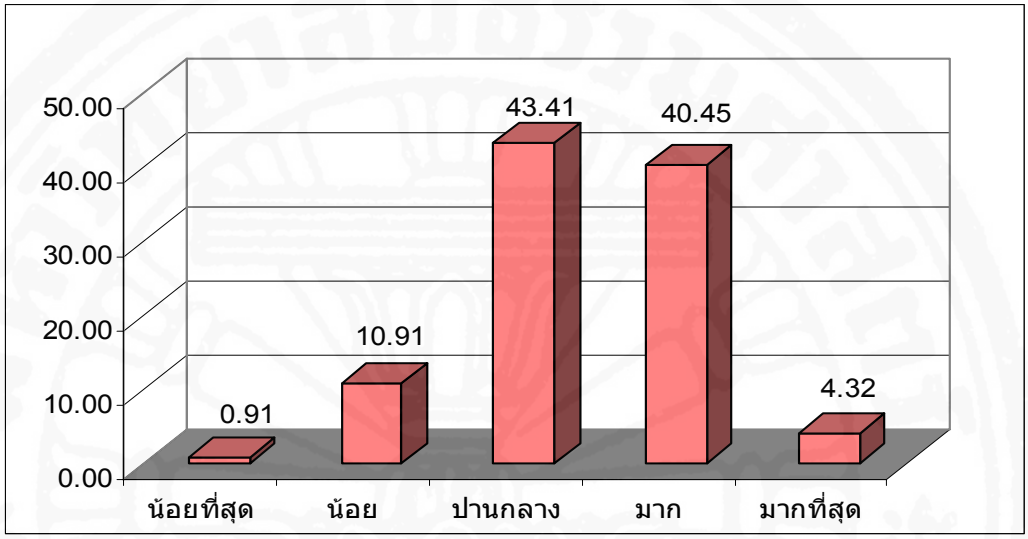
ตารางที่ 4.12

ตารางแสดงผลสำรวจความคิดเห็นด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านคิดว่าปัจจุบันบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่สำคัญ มีความเหมาะสมหรือความปลอดภัยมากน้อยเพียงใด	0	12	43	47	8
ท่านคิดว่าการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยมีความเหมาะสมหรือปลอดภัยมากน้อยเพียงใด	1	13	42	50	4
ท่านมีการระวังและป้องกันอุปกรณ์จากอุบัติเหตุต่างๆมากน้อยเพียงใด เช่น อุบัติเหตุจากการจัดวางคอมพิวเตอร์ในพื้นที่เสี่ยงต่อการเฉี่ยวชน หรือ เสี่ยงต่อการเกิดเข้าใช้งานจากผู้ไม่มีสิทธิ เป็นต้น	1	14	51	38	6
ท่านคิดว่าองค์กรมีการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานมากน้อยเพียงใด	2	9	55	43	1
รวม	4	48	191	178	19
% เฉลี่ยรวม	0.91	10.91	43.41	40.45	4.32

ภาพที่ 4.12

แสดงเปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้านการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมขององค์กร



4.1.2.6 ผลสำรวจด้าน การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)

ตารางที่ 4.13

ผลสำรวจความคิดเห็นด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
หน่วยงานของท่านมีการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures)ตามระยะเวลาอันสมควรสม่ำเสมอมากน้อยเพียงใด	1	29	54	26	0

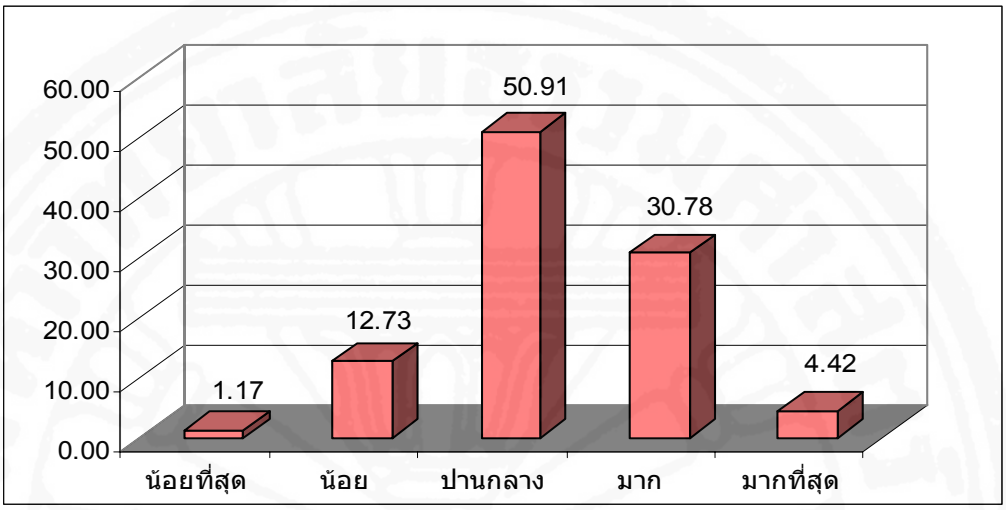
ตารางที่ 4.13 (ต่อ)

ผลสำรวจความคิดเห็นด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านเห็นว่าองค์กรมีการบริหารจัดการเครือข่าย (Network controls)และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application)ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายมีเหมาะสมมากน้อยเพียงใด	1	2	50	51	6
ท่านให้ความสำคัญในการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตหรือไม่เกี่ยวข้องมากน้อยเพียงใด	1	4	44	45	16
ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กร มากน้อยเพียงใด	1	18	58	30	3
ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กรมากน้อยเพียงใด	0	8	65	33	4
ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กรมากน้อยเพียงใด	0	10	63	34	3
ท่านเห็นว่าองค์กรมีการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT สม่ำเสมอมากน้อยเพียงใด	5	27	58	18	2
รวม	9	98	392	237	34
% เฉลี่ยรวม	1.17	12.73	50.91	30.78	4.42

ภาพที่ 4.13

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้านการบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร



4.1.2.7 ผลสำรวจด้าน การควบคุมการเข้าถึง (Access control)

ตารางที่ 4.14

ตารางแสดงผลสำรวจความคิดเห็นด้านการควบคุมการเข้าถึง (Access control)

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กรมากน้อยเพียงใด	1	10	62	37	0
ถ้าองค์กรมีการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ท่านทราบตามระยะที่เหมาะสม(อาจทุก 3 เดือน หรือ 6 เดือน) ท่านเห็นด้วยมากน้อยเพียงใด	4	6	38	48	14
ท่านให้ความสำคัญกับการ Lock Off เครื่อง หรือปิดเครื่อง เมื่อท่านไม่อยู่เป็นเวลานาน เช่น ประชุม, ทานอาหารกลางวัน มากน้อยเพียงใด	8	27	17	40	18

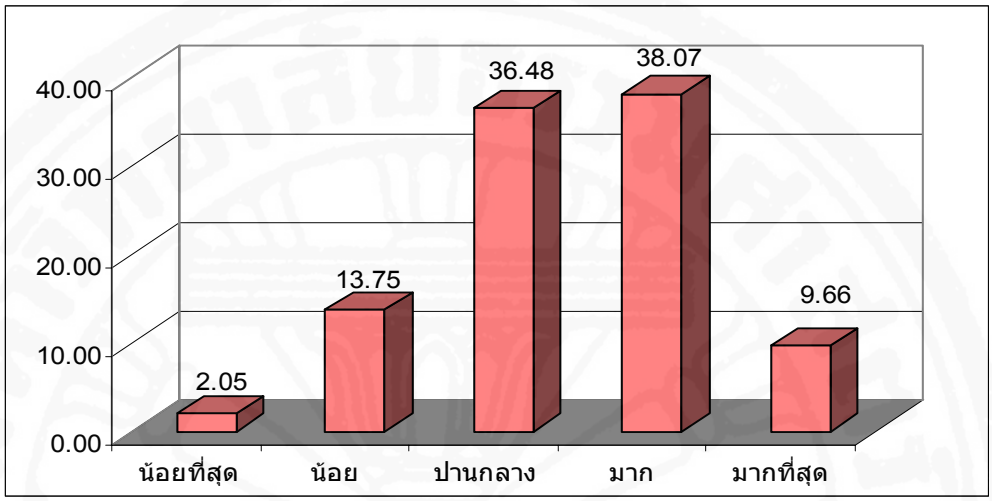
ตารางที่ 4.14 (ต่อ)

ตารางแสดงผลสำรวจความคิดเห็นด้านการควบคุมการเข้าถึง (Access control)

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ท่านใช้งานมากน้อยเพียงใด	0	3	26	58	23
ท่านให้ความสำคัญกับการตั้งUser ID &Password ในโปรแกรมต่างๆขององค์กรมากน้อยเพียงใด	0	5	51	43	11
ท่านเห็นว่ามาตรฐานการใส่ User ID & Password ก่อนเข้าใช้งานระบบต่างๆภายในองค์กร (ระบบบริหารจัดการรหัสผ่าน - Password management system) มีความเหมาะสมและปลอดภัยมากน้อยเพียงใด	0	11	42	49	8
ท่านทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กรมากน้อยเพียงใด เช่น โปรแกรม Photoshop , ACDSee หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์	1	17	42	42	8
ท่านมีการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรมากน้อยเพียงใด ตัวอย่าง การScan ไวรัสใน Handy drive ก่อนใช้งาน ฯลฯ	4	42	43	18	3
รวม	18	121	321	335	85
% เฉลี่ยรวม	2.05	13.75	36.48	38.07	9.66

ภาพที่ 4.14

แสดงเปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้านการควบคุมการเข้าถึง (Access control)



4.1.2.8 ผลสำรวจด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

ตารางที่ 4.15

ผลสำรวจความคิดเห็นด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ผลสำรวจแสดงถึงปริมาณปัญหาที่พบ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านเคยประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลบ้างหรือไม่และมากน้อยเพียงใด (1=ไม่เคย 0%, 2=พบประมาณ1%-25%, 3=พบประมาณ26%-50% , 4 =พบประมาณ51%-75% , 5 = พบประมาณ 76%-100%)	6	19	48	29	8
ท่านเคยประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนบ้างหรือไม่และมากน้อยเพียงใด(1 = ไม่เคย 0%, 2 =พบประมาณ 1%-25%, 3 =พบประมาณ26%-50% , 4 =พบประมาณ51%-75% , 5 =พบประมาณ76%-100%)	8	51	31	15	5

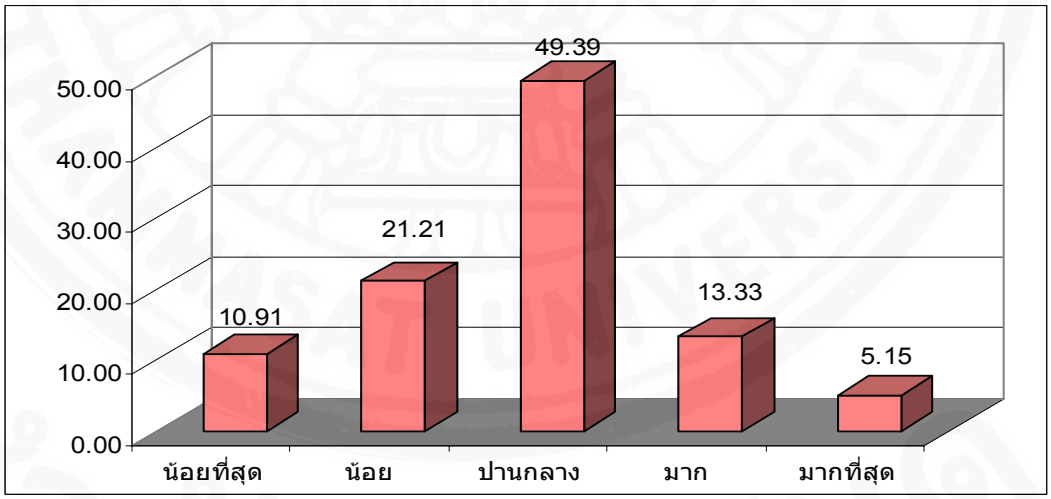
ตารางที่ 4.15

ผลสำรวจความคิดเห็นด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ผลสำรวจแสดงถึงปริมาณปัญหาที่พบ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
เมื่อท่านประสบปัญหาต่างๆดังกล่าวท่านได้ทำการแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดหรือไม่ กรณีผู้ที่ไม่เคยประสบปัญหาใดๆการใช้งานขอให้ข้ามไปข้อต่อไป (1 =แจ้งทุกครั้งที่พบ , 3 = แจ้ง แต่ไม่ทุกครั้ง , 5 = ไม่เคยแจ้ง)	22		84		4
รวม	36	70	163	44	17
% เฉลี่ยรวม	10.91	21.21	49.39	13.33	5.15

ภาพที่ 4.15

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นปริมาณปัญหาที่พบด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ



4.1.2.9 ผลสำรวจด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

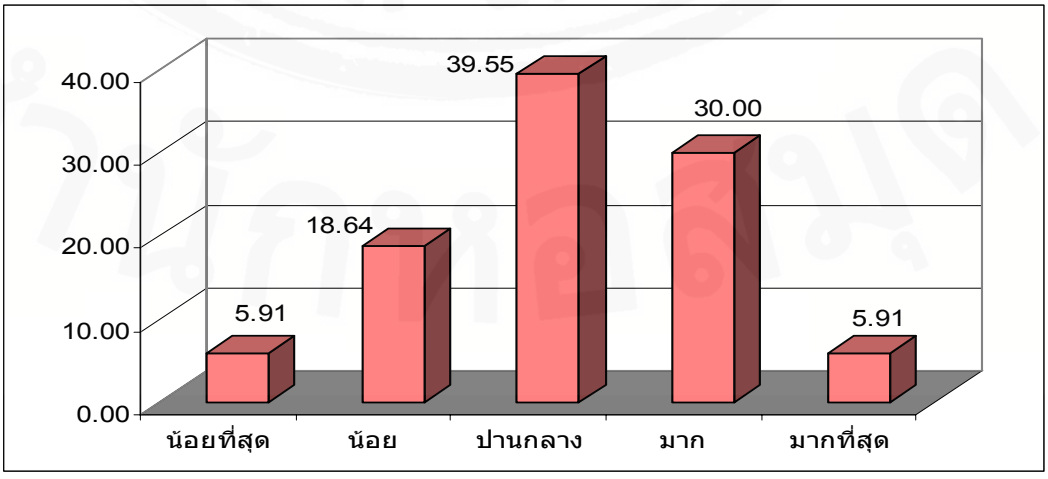
ตารางที่ 4.16

ผลสำรวจความคิดเห็นด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านคิดว่าซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กรมีความเหมาะสมมากน้อยเพียงใด	0	8	49	44	9
ท่านเคยรายงานเหตุการณ์หรือรายงานจุดอ่อนจุดบกพร่องที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่มากน้อยเพียงใด	13	33	38	22	4
รวม	13	41	87	66	13
% เฉลี่ยรวม	5.91	18.64	39.55	30.00	5.91

ภาพที่ 4.16

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร



4.1.2.10 ผลสำรวจด้าน การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

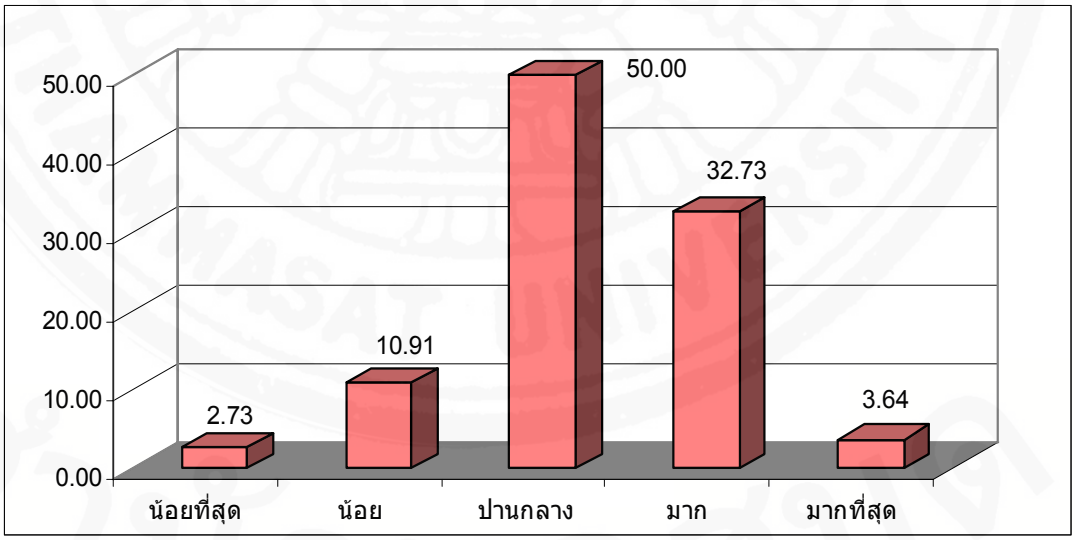
ตารางที่ 4.17

ผลสำรวจความคิดเห็นด้าน การบริหารความต่อเนื่องในการดำเนินงานขององค์กร

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านเห็นว่าปัจจุบันการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมีมากน้อยเพียงใด	3	12	55	36	4
รวม	3	12	55	36	4
% เฉลี่ยรวม	2.73	10.91	50.00	32.73	3.64

ภาพที่ 4.17

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้าน การบริหารความต่อเนื่องในการดำเนินงานขององค์กร



4.1.2.11 ผลสำรวจด้าน การปฏิบัติตามข้อกำหนด (Compliance)

ตารางที่4.18

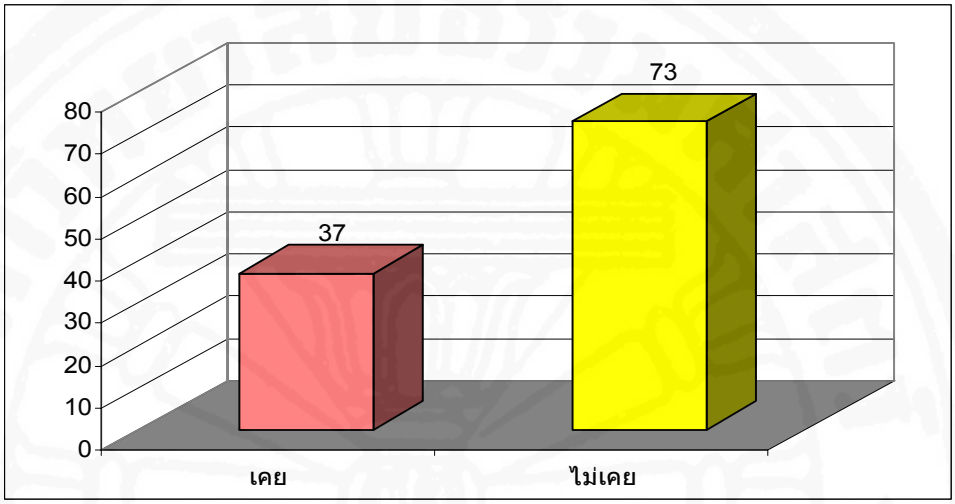
ผลสำรวจความคิดเห็นด้าน การปฏิบัติตามข้อกำหนดขององค์กร

ผลสำรวจ	เคย	ไม่เคย
ท่านเคยลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กรหรือไม่ (1= เคย , 5 = ไม่เคย)	37	73

ผลสำรวจ	น้อยที่สุด	น้อย	ปานกลาง	มาก	มากที่สุด
ท่านเห็นว่าการเข้ารหัสข้อมูล เช่น การเข้าดูข้อมูล การผ่านเข้าออกในส่วนสำคัญต่างๆขององค์กร หรือการเข้าใช้งานอุปกรณ์ต่างๆมีความเข้มงวดและปลอดภัยมากน้อยเพียงใด	1	8	57	42	2
ปัจจุบันผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของท่าน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กรมากน้อยเพียงใด	5	12	54	38	1
รวม	6	20	111	80	3
% เฉลี่ยรวม	2.73	9.09	50.45	36.36	1.36

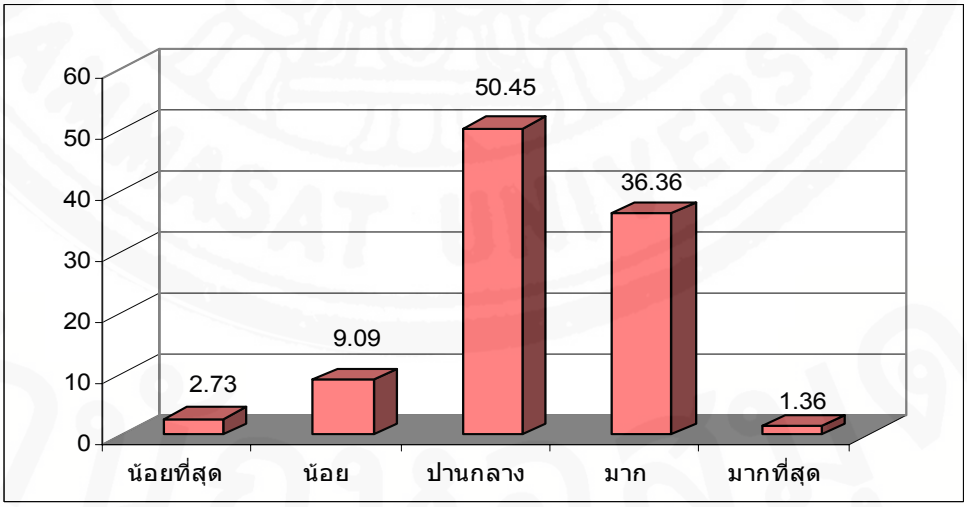
ภาพที่ 4.18

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจผลของการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊กขององค์กร



ภาพที่ 4.19

เปอร์เซ็นต์เฉลี่ยรวมของผลสำรวจความคิดเห็นด้าน การปฏิบัติตามข้อกำหนดขององค์กร



4.1.3 <u>ผลสำรวจความคิดเห็น ด้านการวิเคราะห์ความเสี่ยงของการรักษาความปลอดภัยระบบสารสนเทศ</u>

เป็นผลสำรวจโดยการประเมินความเสี่ยงจากพนักงานในองค์กรโดยแบ่งออก 2 ส่วน คือ

<u>ส่วนที่ 1</u> สำหรับพนักงานทั่วไปทั้งผู้ที่มีหน้าที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT) และผู้ที่ไม่มีหน้าที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Non-IT) เฉพาะในการวิเคราะห์ความเสี่ยงทั่วไปด้าน Confidentiality หรือสิทธิในการเข้าถึงเข้ามูลต่างๆ จำนวนทั้งสิ้น 110 คน ทั้งหมด 3 - ข้อเหตุการณ์ความเสี่ยง

<u>ส่วนที่ 2</u> สำหรับผู้ที่มีหน้าที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT) ขององค์กรโดยตรง จำนวนทั้งสิ้น 44 คน จากผู้สอบแบบสอบถามทั้งหมด 110 คน

โดยสำรวจความคิดเห็นในการวิเคราะห์ ระดับความน่าจะเป็นในการเกิดภัยคุกคามและประเมินผลกระทบเมื่อเกิดเหตุการณ์นั้น ในส่วนที่2 โดยแบ่งภัยคุกคามออกเป็น 3 กลุ่ม คือ สิทธิในการเข้าถึงข้อมูล (Confidentiality) ความถูกต้องและสมบูรณ์ของข้อมูล (Integrity) และการเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้งาน (Availability)

ผลของค่าเฉลี่ยความเสี่ยงที่ได้มาจากผลการคำนวณค่าความเสี่ยงจากความคิดเห็นเรื่องโอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์กรและระดับความรุนแรงของความเสี่ยง (Impact) หากเกิดความเสี่ยงขึ้นนั้นในองค์กร ของกลุ่มตัวอย่าง ตามสูตร

ระดับความเสี่ยง (R) = โอกาสเกิดภัยคุกคาม (L) x ความรุนแรงของผลกระทบ (I)

และนำค่าเฉลี่ยความเสี่ยงไปเปรียบเทียบค่าเพื่อจัดลำดับความเสี่ยงตามตารางเมตริกซ์ ระดับความเสี่ยง 5 x 5 ตารางที่ 4.19

โดยนำระดับความเสี่ยงที่ได้มาแบ่งกลุ่มระดับความเสี่ยงเป็นดังนี้

> 48.00	ความเสี่ยงสูง
= 24.00 – 48.00	ความเสี่ยงปานกลาง
< 24.00	ความเสี่ยงต่ำ

ตารางที่ 4.19

เมตริกซ์ระดับความเสี่ยง 5 x 5

ระดับความรุนแรงของผลกระทบ	ระดับโอกาสในการเกิดเหตุการณ์				
	ประเภท 1 เกิดแน่นอนหรือสูงมาก = 1	ประเภท2 แนวโน้มสูง = 0.8	ประเภท 3 ปานกลาง = 0.6	ประเภท 4 แนวโน้มต่ำ = 0.4	ประเภท 5 ต่ำมากหรือไม่เกิดเลย = 0.2
สูงมาก = 100	100 สูง	80 สูง	60 สูง	40 ปานกลาง	20 ปานกลาง
สูง = 80	80 สูง	64 สูง	48 ปานกลาง	32 ปานกลาง	16 ต่ำ
ปานกลาง = 60	60 สูง	48 ปานกลาง	36 ปานกลาง	24 ปานกลาง	12 ต่ำ
ต่ำ = 40	40 ปานกลาง	32 ปานกลาง	24 ปานกลาง	16 ต่ำ	8 ต่ำ
ต่ำมาก = 20	20 ปานกลาง	16 ต่ำ	12 ต่ำ	8 ต่ำ	4 ต่ำ

จากความคิดเห็นของกลุ่มตัวอย่างพนักงาน สามารถจัดระดับความเสี่ยงของภัยคุกคามแต่ละรูปแบบได้ดังนี้

4.1.3.1 ความเสี่ยงด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล - Confidentiality

ความเสี่ยงเกี่ยวกับการรักษาความลับและความปลอดภัยของข้อมูล และระบบสารสนเทศ หรือความเสี่ยงที่ข้อมูลอาจถูกเปิดเผยหรือใช้โดยที่ไม่ได้รับอนุญาตไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจก็ตาม ข้อมูลต้องจะถูกนำไปใช้โดยบุคคลที่มีสิทธิเข้าใช้ข้อมูลเท่านั้น ช่องโหว่ของความเชื่อถือได้ของข้อมูลสามารถเกิดขึ้นได้เมื่อไม่มีการจัดการเพื่อปกป้องข้อมูลอย่างพอเพียง เช่น ความเสี่ยงจากการเจาะระบบ โครงสร้างการรักษาความปลอดภัย บุคลากรขาดความเอาใจใส่ ผลที่ได้แสดงในตารางที่ 4.20 และ 4.21

ตารางที่ 4.20

ค่าเฉลี่ย โอกาสในการเกิดความเสี่ยง ระดับความรุนแรงของความเสี่ยงและระดับความเสี่ยงด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล (ส่วนที่ 1 จากพนักงานทั้งองค์กร)

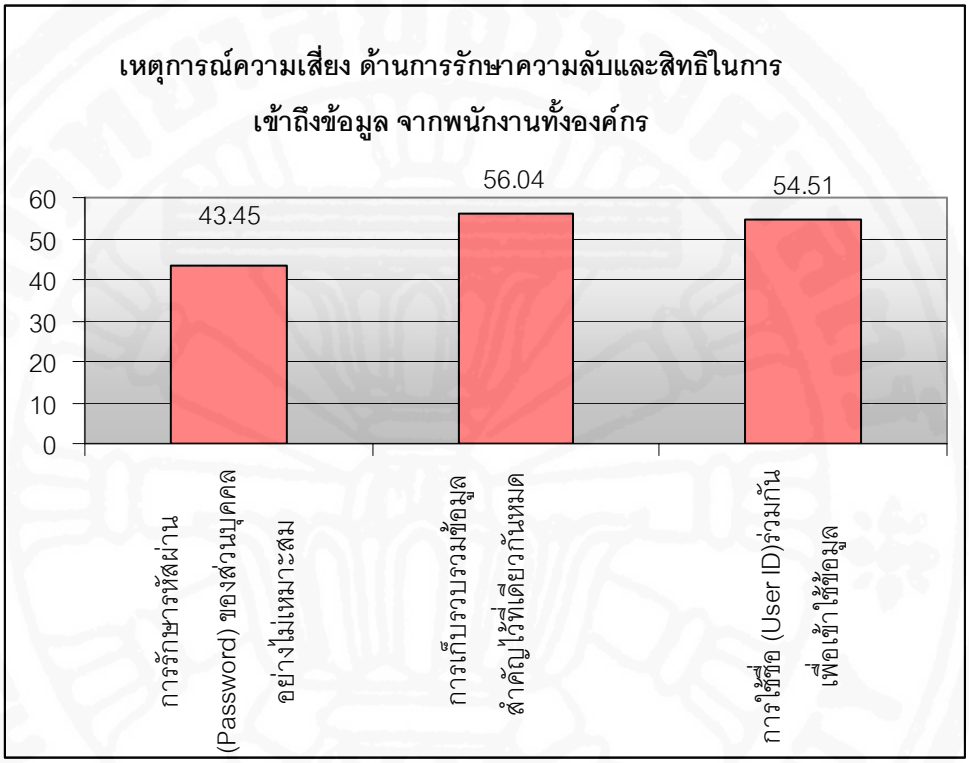
ลำดับที่	เหตุการณ์ความเสี่ยง	ค่าเฉลี่ยโอกาสเกิด	ค่าเฉลี่ยความรุนแรง	ระดับความเสี่ยง
1.	การรักษารหัสผ่าน (Password) ของส่วนบุคคลอย่างไม่เหมาะสม	0.62	68.00	43.45 ปานกลาง
2.	การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด	0.71	76.36	56.04 สูง
3.	การใช้ชื่อ (User ID)ร่วมกันเพื่อเข้าใช้ข้อมูล	0.70	75.64	54.51 สูง

หมายเหตุ เหตุการณ์ความเสี่ยงในด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล สามารถอธิบายคำถามตามแบบสอบถามได้ดังนี้

- การรักษารหัสผ่าน (Password) ของส่วนบุคคลอย่างไม่เหมาะสม เช่น การจดรหัสผ่านติดไว้ที่หน้าจอ การตั้งรหัสผ่านเป็นชื่อหรือนามสกุลตัวเอง เป็นต้น
- การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด เช่น เก็บข้อมูลสำคัญของแผนกไว้ใน database ตัวเดียวกันหมด ซึ่งเสี่ยงเมื่อเกิดความเสียหายต่อ database เครื่องดังกล่าว
- การใช้ชื่อ (User ID)ร่วมกันเพื่อเข้าใช้ข้อมูล หมายถึงการใช้ชื่อหรือสิทธิของผู้อื่นไม่ว่าจะได้รับอนุญาตจากเจ้าของหรือไม่ก็ตาม ในการเข้าใช้ข้อมูลที่ต้องมีการตรวจสอบสิทธิและการพิสูจน์ตัวตน

ภาพที่ 4.20

กราฟค่าเฉลี่ยของความเสี่ยง ด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล ส่วนที่ 1 จากพนักงานทั้งองค์กร



จากผลการสำรวจพนักงานทั้งผู้ที่มีส่วนเกี่ยวข้องกับระบบสารสนเทศและผู้ที่ไม่มีส่วนเกี่ยวข้อง พบว่าระดับความเสี่ยงด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูลส่วนใหญ่อยู่มีความเสี่ยงสูง เรื่อง การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมดและการใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล

ตารางที่ 4.21

ค่าเฉลี่ย โอกาสในการเกิดความเสี่ยง ระดับความรุนแรงของความเสี่ยงและระดับความเสี่ยงด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล (ส่วนที่ 2 เฉพาะพนักงาน IT)

ลำดับที่	เหตุการณ์ความเสี่ยง	ค่าเฉลี่ยโอกาสเกิด	ค่าเฉลี่ยความรุนแรง	ระดับความเสี่ยง
1.1	การเข้าถึงข้อมูลจากผู้ที่ไม่สิทธิใช้งานจริง	0.60	75.00	45.34 ปานกลาง
1.2	การระบุชื่อข้อมูลที่สร้างขึ้นไม่ถูกต้อง	0.59	60.45	35.72 ปานกลาง
1.3	การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง	0.62	61.36	38.21 ปานกลาง
1.4	การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	0.69	74.09	50.85 สูง
1.5	การเข้าใช้ข้อมูลสำรอง (Back up) โดยปราศจากการควบคุม	0.60	75.91	45.20 ปานกลาง

หมายเหตุ เหตุการณ์ความเสี่ยงในด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล สามารถอธิบายคำถามตามแบบสอบถามได้ดังนี้

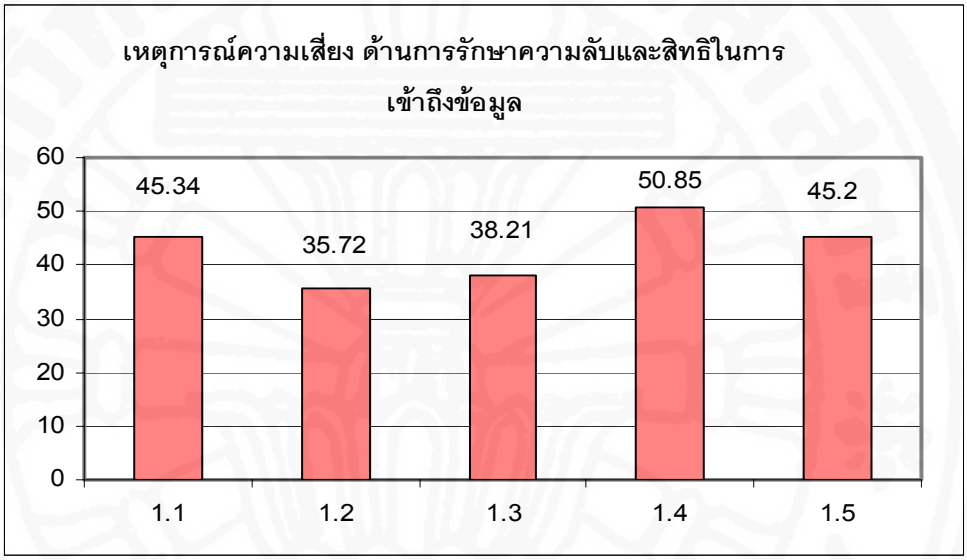
- การเข้าถึงข้อมูลจากผู้ที่ไม่มีสิทธิใช้งานจริง เช่น การเข้าใช้งานโปรแกรมประยุกต์เฉพาะจากผู้ที่ไม่เกี่ยวข้อง การสามารถเรียกดูรายงานที่สำคัญจากผู้ที่ไม่เกี่ยวข้อง
- การระบุชื่อข้อมูลที่สร้างขึ้นไม่ถูกต้อง หมายถึง มีการสร้างข้อมูลแล้วตั้งชื่อข้อมูลไม่ตรงกับข้อมูลจริงหรือกับการใช้งาน เช่น ข้อมูลที่ตั้งชื่อขึ้นต้นด้วยวันที่ที่สร้างข้อมูลเพื่อใช้ในการวิเคราะห์ปัญหา ถูกตั้งชื่อวันที่ผิด
- การจัดเก็บและรักษาข้อมูลแต่ละประเภทไม่ถูกต้อง หมายถึง การไม่สามารถจัดประเภทข้อมูลที่เป็น ข้อมูลลับ(Secret Information),ข้อมูลลับเฉพาะ(Confidential Information), ข้อมูลที่จำเป็นมาก(Critical Information),ข้อมูลสาธารณะหรือข้อมูลทั่วไป จึงอาจเกิดการจัดเก็บหรือรักษา ที่ไม่ถูกต้อง เช่น เก็บข้อมูลทดสอบไว้บนเครื่อง server ที่ใช้งานจริง
- การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม เช่น การพิมพ์ข้อมูลความลับขององค์กรออกนอกบริษัท

- การเข้าใช้ข้อมูลสำรอง (Back up) โดยปราศจากการควบคุม หมายถึง การสามารถเรียกดู หรือนำข้อมูลสำรองออกมาใช้งานโดยไม่ได้รับอนุญาต

ภาพที่ 4.21

กราฟค่าเฉลี่ยของความเสี่ยง ด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล

(ส่วนที่ 2 เฉพาะพนักงาน IT)



จากผลการสำรวจที่ได้พบระดับความเสี่ยงด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูลส่วนใหญ่อยู่ในระดับปานกลาง และที่มีความเสี่ยงสูง คือ เรื่องการพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม ซึ่งองค์กรควรให้ความสำคัญและลงทำความเข้าใจกับผู้ใช้งาน เพื่อสร้างความตระหนักด้านความปลอดภัยของข้อมูลต่างๆภายในองค์กร

4.1.3.2 ความเสี่ยงด้านความถูกต้องและความครบถ้วนของข้อมูล - Integrity

ความเสี่ยงที่ข้อมูลอาจไม่ถูกต้องและครบถ้วน อาจเกิดจากจากการนำข้อมูลที่ผิดพลาดเข้าสู่ระบบ หรือการประมวลผลที่ไม่ถูกต้อง ซึ่งส่งผลกระทบต่อการดำเนินธุรกิจ เนื่องจากการใช้ข้อมูลที่ไม่ถูกต้องนั้น

ผลจากแบบสอบถามในการสำรวจความคิดเห็นจากกลุ่มตัวอย่างได้ค่าเฉลี่ยความเสี่ยงและระดับความเสี่ยงดังตารางที่ 4.22

ตารางที่ 4.22

แสดงค่าเฉลี่ย โอกาสในการเกิดความเสี่ยง ระดับความรุนแรงของความเสี่ยงและระดับความเสี่ยงด้านความถูกต้องและสมบูรณ์ของข้อมูล (ส่วนที่ 2 เฉพาะพนักงาน IT)

ลำดับที่	เหตุการณ์ความเสี่ยง	ค่าเฉลี่ยโอกาสเกิด	ค่าเฉลี่ยความรุนแรง	ระดับความเสี่ยง
2.1	การเกิดความผิดพลาดในการรายงานข้อมูล	0.63	73.18	46.09 ปานกลาง
2.2	ข้อมูลภายในองค์กรขาดการพัฒนาหรืออัพเดท (Update)ให้ทันสมัย	0.62	65.91	42.00 ปานกลาง
2.3	ฐานข้อมูล(database)ถูกขัดจังหวะการทำงาน (corrupt)เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด	0.62	77.27	49.27 สูง
2.4	ระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบสิทธิการใช้งานไม่มีการเปลี่ยนแปลงให้ทันสมัย	0.59	73.64	44.45 ปานกลาง
2.5	การขาดกระบวนการภายในเพื่อจัดการ,สร้าง, และควบคุมข้อมูลภายในองค์กร	0.61	66.36	41.64 ปานกลาง
2.6	การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์ (application) ระบบ(system) หรือ ซอฟแวร์ (Software)ที่มีการแก้ไขเปลี่ยนแปลง	0.64	69.09	45.18 ปานกลาง
2.7	มีการแก้ไขโปรแกรมประยุกต์ (Application)อย่างไม่ถูกต้อง	0.62	73.18	46.18 ปานกลาง
2.8	กระบวนการควบคุมต่างๆมีความซับซ้อนเกินไปผู้ใช้งานจึงไม่ให้ความใส่ใจ	0.57	61.82	35.36 ปานกลาง

หมายเหตุ เหตุการณ์ความเสี่ยงในด้านความถูกต้องและความครบถ้วนของข้อมูล สามารถอธิบายคำถามตามแบบสอบถามได้ดังนี้

- ความผิดพลาดในการรายงานข้อมูล เช่น การประมวลผลข้อมูลในระบบผิดพลาด ดังนั้นเมื่อผู้ใช้งานนำข้อมูลออกจากระบบไปใช้ ทำให้เกิดปัญหาต่อผู้ใช้ข้อมูล

- ข้อมูลภายในองค์กรขาดการพัฒนาหรืออัพเดท(Update)ให้ทันสมัยให้เป็นเวอร์-ชั่นล่าสุด เช่น การไม่มีการอัพเดทโปรแกรมบน Server เป็นต้น

- ฐานข้อมูล(database)ถูกขัดจังหวะการทำงาน(corrupt)เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด หมายถึง การที่เครื่อง Server เกิดขัดข้องทำให้ database บนเครื่อง server ดังกล่าวหยุดการทำงานชั่วขณะ ทำให้ข้อมูลในช่วงเวลาดังกล่าวไม่ถูกเก็บลง database และทำให้การทำงานที่เกี่ยวข้องต้องหยุดตาม

- ระบบรักษาความปลอดภัยของข้อมูลและขั้นตอนการตรวจสอบสิทธิการใช้งานไม่มีการเปลี่ยนแปลงให้ทันสมัย

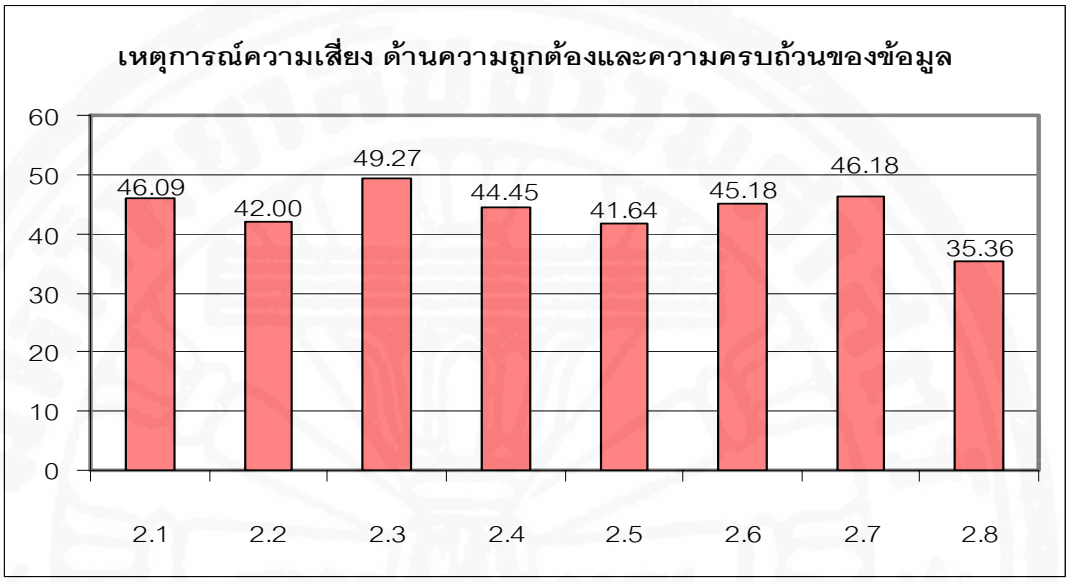
- การขาดกระบวนการภายในเพื่อจัดการ,สร้าง,และควบคุมข้อมูลภายในองค์กร หมายถึง การที่องค์กรขาดระบบในการจัดการข้อมูล ทำให้ควบคุมการใช้ข้อมูลเป็นไปอย่างลำบาก

- การขาดการเก็บบันทึกข้อมูล โปรแกรมประยุกต์(application) ระบบ(system) หรือ ซอฟแวร์(Software)ที่มีการแก้ไขเปลี่ยนแปลง) หมายถึง เมื่อมีการแก้ไขหรือเปลี่ยนแปลงข้อมูลบนระบบ แล้วไม่มีการทำบันทึกหรือแจ้งผู้เกี่ยวข้องทราบ ดังนั้นเมื่อเกิดปัญหาขึ้นจะไม่สามารถตรวจสอบย้อนกลับได้ว่าเกิดจากสาเหตุใด

- มีการแก้ไขโปรแกรมประยุกต์(Application)อย่างไม่ถูกต้อง เช่น แก้ไขรหัส (code) โดยไม่มีการทดสอบ

- กระบวนการควบคุมต่างๆมีความซับซ้อนเกินไป ผู้ใช้งานจึงไม่ให้ความใส่ใจ เช่น การสร้างเงื่อนไขในการใช้ข้อมูลให้มีหลายขั้นตอน ทำให้ผู้ใช้งานพยายามหาวิธีอื่นที่ง่ายกว่ามาแอบใช้ข้อมูล

ภาพที่ 4.22
กราฟค่าเฉลี่ยของความเสี่ยง ด้านความถูกต้องและความครบถ้วนของข้อมูล
(ส่วนที่ 2 เฉพาะพนักงาน IT)



จากผลการสำรวจที่ได้พบระดับความเสี่ยงด้านความถูกต้องและความครบถ้วนของข้อมูลส่วนใหญ่อยู่ในระดับปานกลาง และที่มีความเสี่ยงสูง คือ เรื่องฐานข้อมูล (Database) ถูกขัดจังหวะการทำงาน (corrupt) เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด

ซึ่งความเสี่ยงดังกล่าวจะส่งผลถึงทั้งผู้ใช้งานภายในและภายนอกองค์กรเนื่องจากเมื่อการที่เครื่อง Server เกิดขัดข้องทำให้ database บนเครื่อง server ดังกล่าวหยุดการทำงานชั่วขณะ ทำให้ข้อมูลในช่วงเวลาดังกล่าวไม่ถูกเก็บลงdatabase ทำให้การทำงานที่เกี่ยวข้องต้องหยุดตาม ดังนั้นถ้าขณะก่อนหยุดเป็นช่วงที่ผู้ใช้งานกำลังใช้งานหรือทำธุรกรรมที่สำคัญอยู่บนระบบ เมื่อระบบหยุด ข้อมูลดังกล่าวไม่ถูกเก็บ ผู้ใช้งานย่อมเกิดความไม่พอใจและเกิดปัญหาเรื่องข้อมูลที่ขาดหายไปหรือผิดพลาดตามมา

4.1.3.3 <u>ความเสี่ยงด้านการเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้งาน - Availability</u>

ความเสี่ยงด้านความสามารถในการใช้งานเมื่อต้องการข้อมูล เป็นความเสี่ยงที่ระบบสารสนเทศหยุดชะงักและไม่สามารถให้บริการกับธุรกิจได้อย่างต่อเนื่อง เมื่อจะต้องนำข้อมูลมาใช้งาน ทำให้ผู้มีสิทธิใช้ข้อมูลไม่สามารถนำข้อมูลไปใช้งานได้ เช่น ความเสี่ยงเกี่ยวกับอุบัติภัย อุบัติเหตุ เทคโนโลยีที่ล้าสมัย การไม่มีแผนฉุกเฉิน และระบบเครือข่าย เป็นต้น

ผลจากแบบสอบถามในการสำรวจความคิดเห็นจากกลุ่มตัวอย่างได้ค่าเฉลี่ยความเสี่ยงและระดับความเสี่ยงดังตารางที่ 4.23

ตารางที่ 4.23

ค่าเฉลี่ย โอกาสในการเกิดความเสี่ยง ระดับความรุนแรงของความเสี่ยงและระดับความเสี่ยงด้านการเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้งาน (ส่วนที่ 2 เฉพาะพนักงาน IT)

ลำดับที่	เหตุการณ์ความเสี่ยง	ค่าเฉลี่ยโอกาสเกิด	ค่าเฉลี่ยความรุนแรง	ระดับความเสี่ยง
3.1	ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้	0.60	80.91	50.73 สูง
3.2	การออกแบบระบบซับซ้อนเกินไป	0.57	64.55	37.45 ปานกลาง
3.3	การติดตั้งฮาร์ดแวร์หรือซอฟแวร์ไม่ถูกต้อง	0.53	60.45	32.64 ปานกลาง
3.4	ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย	0.61	67.27	42.45 ปานกลาง
3.5	การดูแลรักษา(maintenance)ระบบ ทำให้ระบบไม่สามารถใช้งานได้	0.60	74.09	45.09 ปานกลาง
3.6	งบประมาณในการสำรอง (Back up) ข้อมูลไม่เพียงพอ	0.60	70.00	42.45 ปานกลาง
3.7	พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม	0.58	67.27	39.64 ปานกลาง
3.8	Router / Firewall เสียทำให้ไม่สามารถใช้งานได้	0.61	80.91	50.36 สูง
3.9	ข้อมูลที่เก็บสำรอง (Back up)ไม่เพียงพอ	0.60	72.27	44.91 ปานกลาง
3.10	การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้	0.63	84.09	55.09 สูง

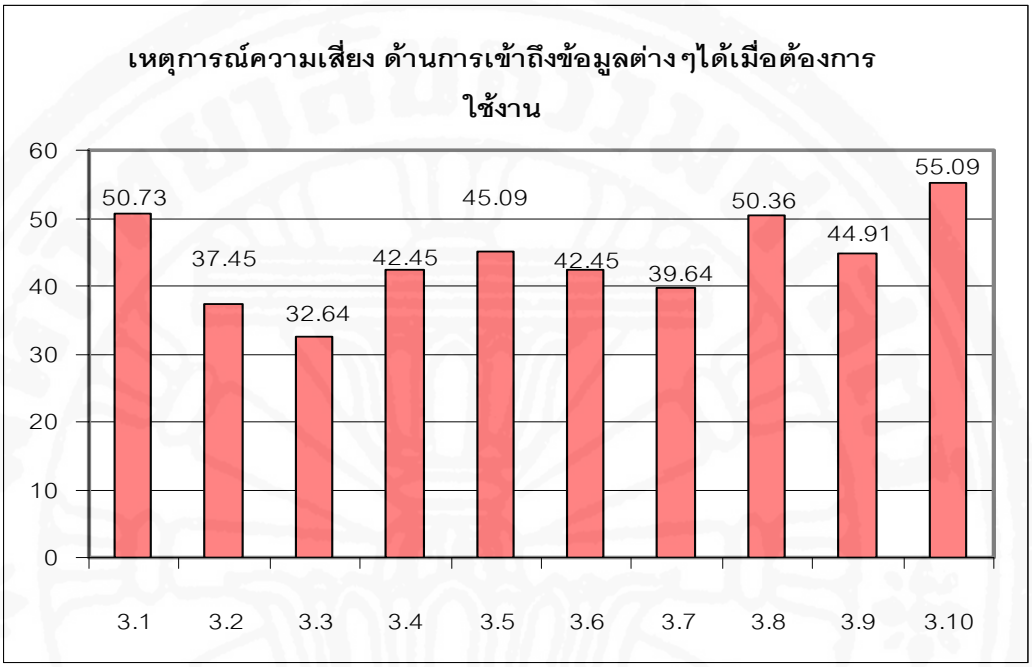
หมายเหตุ เหตุการณ์ความเสี่ยงในด้านการเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้งาน สามารถอธิบายคำถามตามแบบสอบถามได้ดังนี้

- ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้ หมายถึงการถูกบุกรุกโดยการเจาะระบบรักษาความปลอดภัยเข้ามาถึงเครื่อง server ภายในองค์กรได้ไม่ว่าจะด้วยเทคนิคหรือวิธีใดก็ตาม
- การออกแบบระบบซับซ้อนเกินไป จนอาจเกินความจำเป็นในการใช้งานและเกิดความซับซ้อนจนเกินไป
- การติดตั้งฮาร์ดแวร์หรือซอฟแวร์ไม่ถูกต้อง จึงเกิดความเสี่ยงต่อการใช้งาน และระบบที่เกี่ยวข้อง
- ปริมาณการใช้งานที่เข้ามาโดยไม่คาดหมาย เช่น ลูกค้าภายนอกเข้าใช้งานและดูข้อมูลใน website ขององค์กรจำนวนมากในเวลาเดียวกันจนระบบล่ม
- การดูแลรักษา (maintenance) ระบบทำให้ระบบไม่สามารถใช้งานได้ (unavailable) หมายถึงการที่ผู้ดูแลระบบทำการตรวจสอบและปิดเครื่อง server ในช่วงเวลาที่มีการใช้งานของผู้ใช้ จึงเกิดการขัดจังหวะในการทำงาน
- งบประมาณในการสำรอง (Back up) ข้อมูลไม่เพียงพอ หมายถึง การขาดงบประมาณสำหรับค่าใช้จ่ายของอุปกรณ์และการติดตั้งการวางระบบสำรองข้อมูลขององค์กร
- พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม หมายถึง การที่พนักงานขาดการสร้างความรู้ความเข้าใจในการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศขององค์กร การไม่ได้รับการอบรมความรู้ใหม่เมื่อมีการเปลี่ยนแปลงรูปแบบการทำงานหรือระบบที่ใช้งานจากแบบเดิม
- Router / Firewall เสียทำให้ไม่สามารถใช้งานได้ หมายถึง การที่ระบบเกิดความไม่ปลอดภัย เนื่องจากอุปกรณ์เครือข่ายขัดข้องทำให้การเชื่อมต่อไปยังข้อมูลที่ต้องการถูกตัดขาดและเสี่ยงต่อการถูกบุกรุกจากผู้ไม่ประสงค์ดี
- ข้อมูลที่เก็บสำรอง (Back up) ไม่เพียงพอ หมายถึงไม่ได้มีการสำรองข้อมูลแบบทั้งหมด (Full Backup) ทำให้เกิดปัญหาเมื่อต้องการข้อมูลส่วนที่ไม่ได้ทำการสำรองข้อมูลไว้
- การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้ หมายถึง กรณีลูกค้าไม่สามารถเข้าใช้งานหรือดูข้อมูลที่ต้องการ และเกิดความไม่พอใจต่อการใช้งาน

ภาพที่ 4.23

กราฟแสดงค่าเฉลี่ยของความเสี่ยง ด้านการเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้งาน

(ส่วนที่ 2 เฉพาะพนักงาน IT)



จากผลการสำรวจที่ได้พบระดับความเสี่ยงด้านด้านการเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้งาน ส่วนใหญ่อยู่ในระดับปานกลาง และที่มีความเสี่ยงสูงมี 3 เรื่อง คือ

- ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้
- Router / Firewall เสียทำให้ไม่สามารถใช้งานได้
- การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้

ซึ่งทั้ง 3 เรื่องมีความสัมพันธ์กัน เพราะเมื่อ Router / Firewall เสียทำให้ไม่สามารถใช้งานได้แล้วย่อมอาจก่อให้เกิดการบุกรุกจากผู้ที่ไม่สิทธิ เพื่อเข้ามาทำความเสียหายต่อระบบหรือข้อมูลต่างๆ เพราะตัวป้องกันหยุดทำงาน และเมื่อระบบเกิดความเสียหาย ลูกค้าก็ไม่สามารถเข้าใช้งานระบบที่ให้บริการได้เช่นกัน จึงเกิดผลกระทบต่อความพึงพอใจและรายได้ขององค์กร

จากการประเมินความเสี่ยงทั้ง 3 ด้านแล้วนั้นพบความเสี่ยงระดับสูงที่องค์กร ควรเร่งในการเอาใจใส่เป็นพิเศษ ในการหาแนวทางการแก้ปัญหาหรือพัฒนาปรับปรุง โดยเหตุการณ์ความเสี่ยงที่ได้ จากการสำรวจความคิดเห็นของกลุ่มตัวอย่าง ที่พบว่ามีระดับความเสี่ยงสูง มีจำนวน 7 เหตุการณ์ เรียงลำดับได้ตาม ตารางที่ 4.24

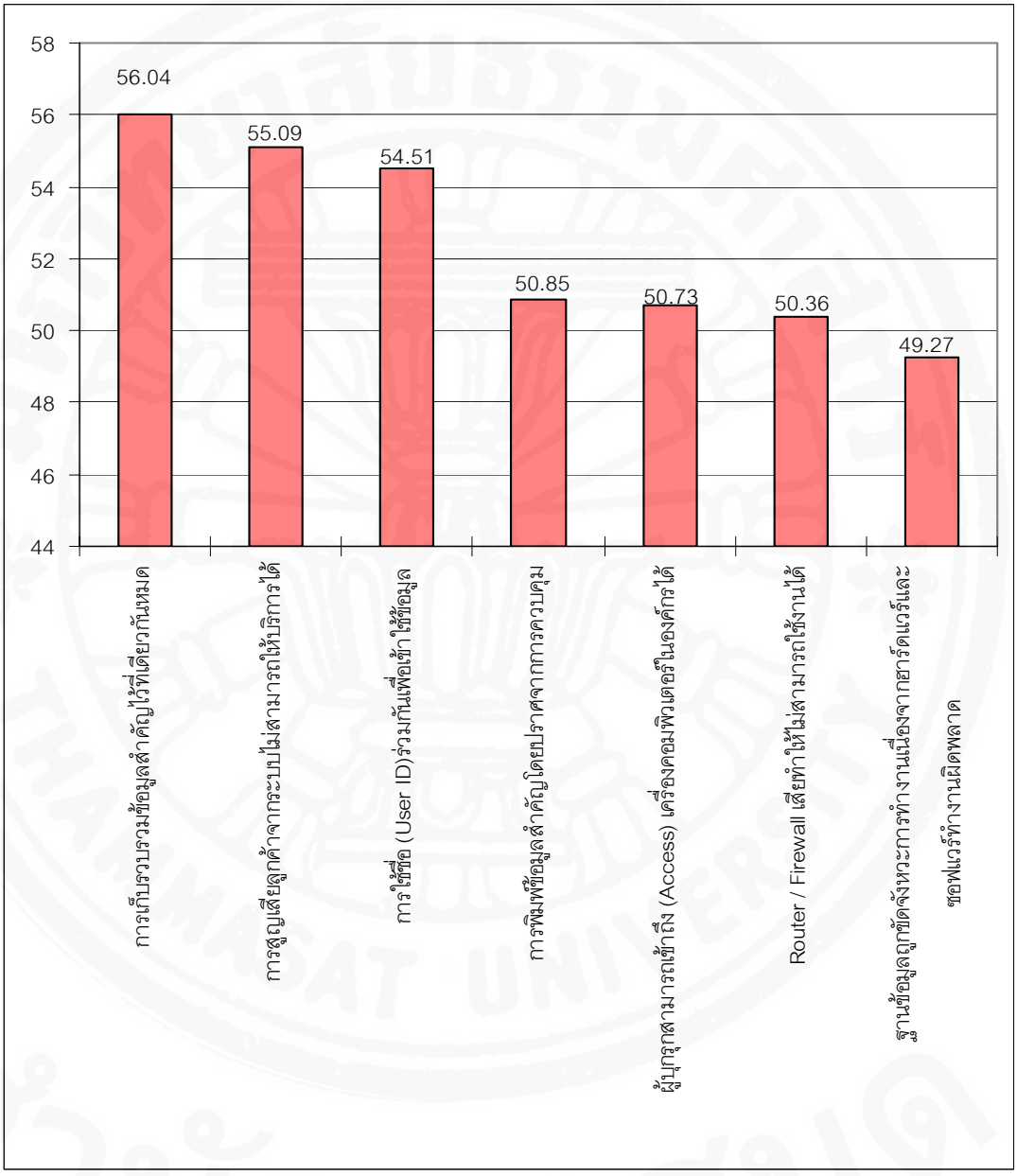
ตารางที่ 4.24

ลำดับของระดับความเสี่ยงของเหตุการณ์ที่ก่อให้เกิดความเสี่ยงต่อองค์กรในการรักษาความปลอดภัยด้านสารสนเทศ

ลำดับที่	เหตุการณ์ที่ก่อให้เกิดความเสี่ยงต่อองค์กรในการรักษาความปลอดภัยด้านสารสนเทศ	ระดับความเสี่ยง	ประเภทของความเสี่ยง
1	การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด	56.04 สูง	Confidentiality
2	การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้	55.09 สูง	Availability
3	การใช้ชื่อ (User ID)ร่วมกันเพื่อเข้าใช้ข้อมูล	54.51 สูง	Confidentiality
4	การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม	50.85 สูง	Confidentiality
5	ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้	50.73 สูง	Availability
6	Router / Firewall เสียทำให้ไม่สามารถใช้งานได้	50.36 สูง	Availability
7	ฐานข้อมูล(database)ถูกขัดจังหวะการทำงาน (corrupt)เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด	49.27 สูง	Integrity

ภาพที่ 4.24

กราฟลำดับของระดับความเสี่ยงของเหตุการณ์ที่ก่อให้เกิดความเสี่ยงต่อองค์กรในการรักษาความปลอดภัยด้านสารสนเทศ



4.2 ผลการทดสอบสมมุติฐาน

จากผลสำรวจความคิดเห็นเรื่องความปลอดภัยด้านสารสนเทศภายในองค์กรที่ให้บริการ ด้านการจัดซื้อออนไลน์(e-Procurement) ผลที่ได้สามารถนำมาประมวลผลและทดสอบสมมติฐานได้ดังนี้

4.2.1 สมมติฐานข้อที่ 1

ระยะอายุเวลาการทำงานของพนักงานมีความสัมพันธ์ต่อความคิดเห็นเรื่องความปลอดภัยด้านสารสนเทศไม่แตกต่างอย่างมีนัยสำคัญ แยกเป็นรายข้อตามมาตรฐาน ISO 17799 จำนวน 11 ข้อใหญ่จากการทดสอบทางสถิติแบบ One way ANOVA เป็นดังนี้

4.2.1.1 ผลสำรวจด้าน นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงานในองค์กรปัจจุบันเป็นดังตารางที่ 4.25 และภาพที่ 4.25

ตารางที่ 4. 25

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่1และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะอายุเวลาการทำงานต่างๆ

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร	<1 ปี	19	2.8947	2.05196
	1-2 ปี	47	3.6383	1.91590
	3-4 ปี	25	3.8800	1.83303
	>4 ปี	19	4.5789	1.26121
	รวม	110	3.7273	1.87161
2. การทราบรายละเอียดของนโยบาย	<1 ปี	19	1.4211	1.26121
	1-2 ปี	47	3.0426	2.02116

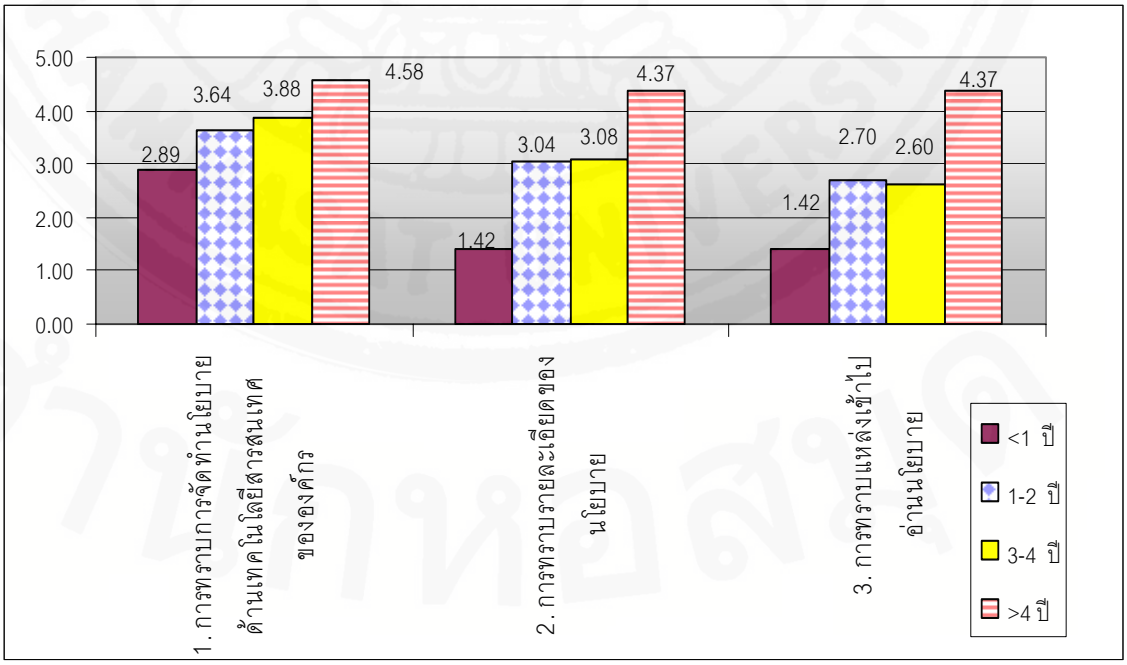
ตารางที่ 4. 25 (ต่อ)

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่1และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะอายุเวลาการทำงานต่างๆ

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
2. การทราบรายละเอียดของนโยบาย	3-4 ปี	25	3.0800	2.03961
	>4 ปี	19	4.3684	1.49854
	รวม	110	3.0000	2.00915
3. การทราบแหล่งที่สามารถเข้าไปอ่านนโยบาย	<1 ปี	19	1.4211	1.26121
	1-2 ปี	47	2.7021	1.99907
	3-4 ปี	25	2.6000	2.00000
	>4 ปี	19	4.3684	1.49854
	รวม	110	2.7455	1.99281

ภาพที่ 4.25

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่1 แยกเป็นช่วงระยะอายุเวลาการทำงานต่างๆ



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่1 จำแนกตามแยกเป็นช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆมีความมีความคิดเห็นต่อการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กร มีค่า 0.044 (Sig. = 0.044) ซึ่งน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงานที่ต่ำกว่า 1 ปี กับช่วงอายุงานที่มากกว่า 4 ปี

(2) ความคิดเห็นต่อการทราบรายละเอียดของนโยบายขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบรายละเอียดของนโยบายขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบรายละเอียดของนโยบายขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบรายละเอียดของนโยบายขององค์กร มีค่า 0.000 (Sig. = 0.000) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงสมมติฐาน H_0

และยอมรับสมมติฐานปฏิเสธ H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบรายละเอียดของนโยบายขององค์กรแตกต่างกัน อย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องการทราบรายละเอียดของนโยบายขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ

ช่วงอายุ < 1 ปี กับ ช่วง 1-2 ปี, ช่วงอายุ < 1 ปี กับ ช่วง 3-4 ปี, ช่วงอายุ < 1 ปี กับ ช่วง >4 ปี

(3) ความคิดเห็นต่อการรทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กร มีค่า 0.000 (Sig. = 0.000) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆมีความคิดเห็นต่อการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กรแตกต่างกัน

โดยคู่ที่แตกต่างกันเรื่องการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ

ช่วงอายุ >4 ปี กับ ช่วง 1-2 ปี, ช่วงอายุ >4 ปี กับ ช่วง 3-4 ปี, ช่วงอายุ < 1 ปี กับ ช่วง >4 ปี

4.2.1.2 <u>ผลสำรวจด้าน โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงาน เป็นดังตารางที่ 4.26 และภาพที่ 4.26

ตารางที่ 4.26

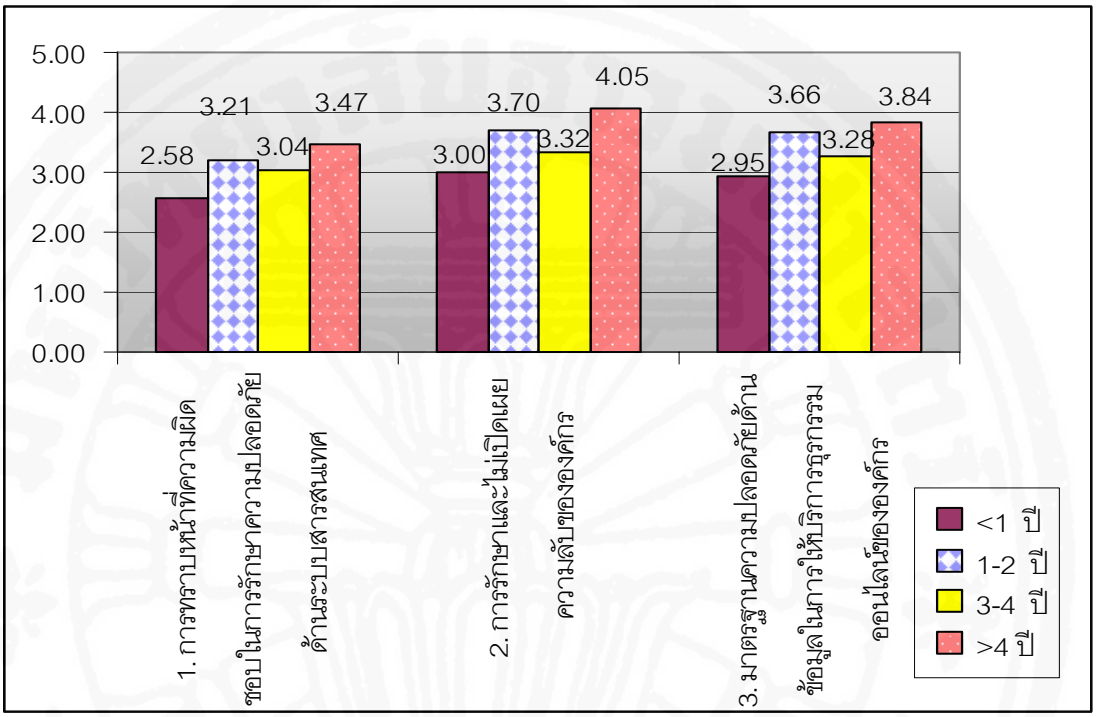
ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่2 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะอายุเวลาการทำงานต่างๆ

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศ	<1 ปี	19	2.5789	.69248
	1-2 ปี	47	3.2128	.83239
	3-4 ปี	25	3.0400	1.01980
	>4 ปี	19	3.4737	.84119
	รวม	110	3.1091	.89181
2. การรักษาและไม่เปิดเผยความลับขององค์กร	<1 ปี	19	3.0000	.57735
	1-2 ปี	47	3.7021	.97613
	3-4 ปี	25	3.3200	1.14455
	>4 ปี	19	4.0526	.77986
	รวม	110	3.5545	.98229
3. มาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กร	<1 ปี	19	2.9474	.91127
	1-2 ปี	47	3.6596	.66844
	3-4 ปี	25	3.2800	.73711
	>4 ปี	19	3.8421	.83421
	รวม	110	3.4818	.80971

ภาพที่ 4. 26

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 2

ตามช่วงระยะอายุเวลาการทำงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่2 จำแนกตามช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กร มีค่า 0.012 (Sig. = 0.012) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่าระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงานที่ต่ำกว่า 1 ปี กับช่วงอายุงานที่มากกว่า 4 ปี

(2) ความคิดเห็นต่อการรักษาและไม่เปิดเผยความลับขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการรักษาและไม่เปิดเผยความลับขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการรักษาและไม่เปิดเผยความลับขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการรักษาและไม่เปิดเผยความลับขององค์กร มีค่า 0.003 (Sig. = 0.003) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่าระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการรักษาและไม่เปิดเผยความลับขององค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องการรักษาและไม่เปิดเผยความลับขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffeคือ ช่วงอายุงานที่ต่ำกว่า 1 ปี กับช่วงอายุงานที่มากกว่า 4 ปี

(3) ความคิดเห็นต่อมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กร

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กร มีค่า 0.001 (Sig. = 0.001) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ

ช่วงอายุ < 1 ปี กับ ช่วง 1-2 ปีและ ช่วงอายุ < 1 ปี กับ ช่วง >4 ปี

4.2.1.3 ผลสำรวจด้าน หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงาน เป็นดังตารางที่ 4.27 และภาพที่ 4.27

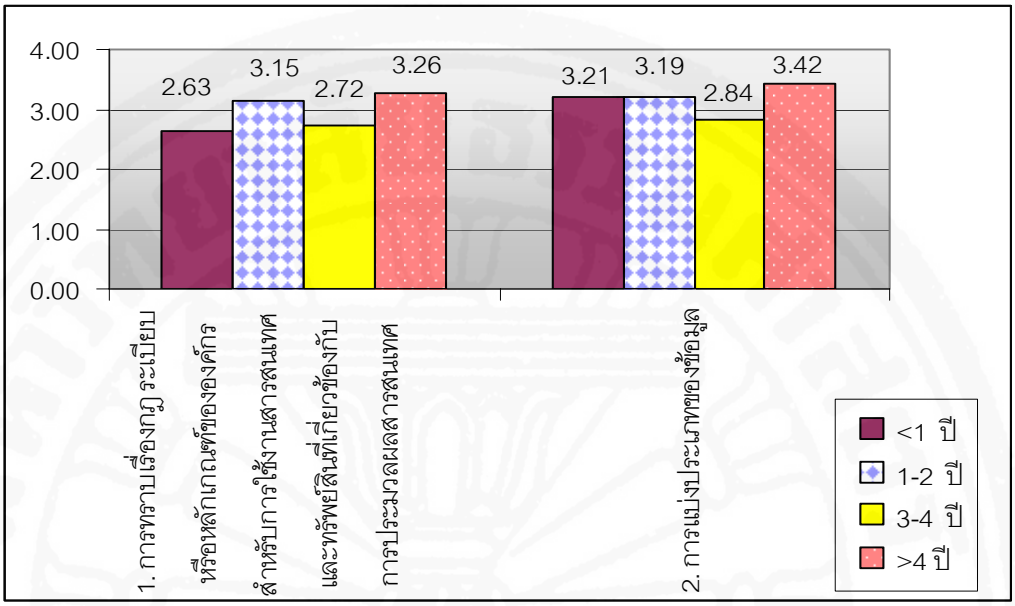
ตารางที่ 4. 27

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่3และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ	<1 ปี	19	2.6316	.76089
	1-2 ปี	47	3.1489	.58898
	3-4 ปี	25	2.7200	.93630
	>4 ปี	19	3.2632	.65338
	รวม	110	2.9818	.75397
2. การแบ่งประเภทของข้อมูล	<1 ปี	19	3.2105	.63060
	1-2 ปี	47	3.1915	.61284
	3-4 ปี	25	2.8400	.80000
	>4 ปี	19	3.4211	1.01739
	รวม	110	3.1545	.75646

ภาพที่ 4.27

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 3
แยกเป็นช่วงระยะเวลาการทำงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่3 จำแนกตามช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ มีค่า 0.006 (Sig. = 0.006) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่าระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบ

เรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศแตกต่างกันอย่างน้อย 1 คู่

แต่เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe กับไม่พบคู่ที่แตกต่างกัน

(2) ความคิดเห็นต่อการแบ่งประเภทของข้อมูล

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการแบ่งประเภทของข้อมูลไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการแบ่งประเภทของข้อมูลแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการความคิดเห็นต่อการแบ่งประเภทของข้อมูล มีค่า 0.073 (Sig. = 0.073) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการแบ่งประเภทของข้อมูลไม่แตกต่างกัน

4.2.1.4 <u>ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงาน เป็นดังตารางที่ 4.28 และภาพที่ 4.28

ตารางที่ 4.28

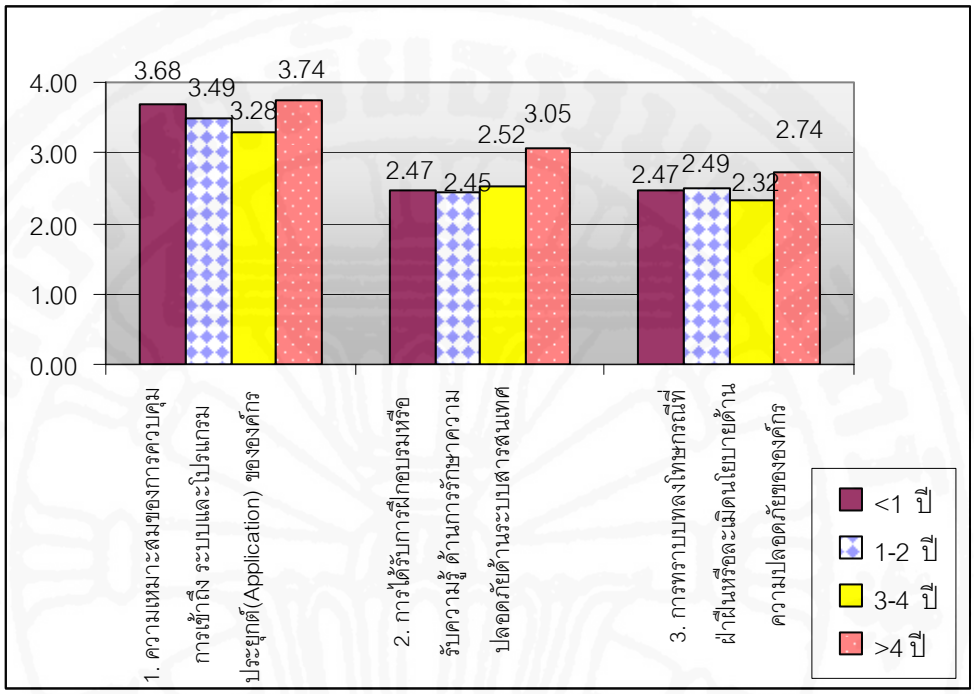
ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 4 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. ความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์(Application) ขององค์กร	<1 ปี	19	3.6842	0.94591
	1-2 ปี	47	3.4894	0.50529
	3-4 ปี	25	3.2800	0.79162
	>4 ปี	19	3.7368	0.73349
	รวม	110	3.5182	0.71333
2. การได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศ	<1 ปี	19	2.4737	1.07333
	1-2 ปี	47	2.4468	0.85487
	3-4 ปี	25	2.5200	0.71414
	>4 ปี	19	3.0526	0.84811
	รวม	110	2.5727	0.88265
3. การทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กร	<1 ปี	19	2.4737	0.69669
	1-2 ปี	47	2.4894	0.88151
	3-4 ปี	25	2.3200	0.80208
	>4 ปี	19	2.7368	1.09758
	รวม	110	2.4909	0.87520

ภาพที่ 4.28

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 4

แยกเป็นช่วงระยะเวลาการทำงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่4 จำแนกตามช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์(Application) ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์ (Application) ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์ (Application) ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์ (Application) ขององค์กร มีค่า 0.127 (Sig. = 0.127) มีค่ามากกว่าระดับ

นัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้าถึงระบบและโปรแกรมประยุกต์ (Application) ขององค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อการได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศ

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อการได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อการได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการได้รับการฝึกอบรมหรือรับความรู้ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศ มีค่า 0.073 (Sig. = 0.073) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อการได้รับการฝึกอบรมหรือรับความรู้ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศไม่แตกต่างกัน

(3) ความคิดเห็นต่อการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กร มีค่า 0.488 (Sig. = 0.488) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่าระยะอายุของเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กรไม่แตกต่างกัน

4.2.1.5 ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

พบว่าค่าความคิดเห็นตามช่วงระยะเวลาการทำงาน ดังตารางที่ 4.29และภาพที่ 4.29

ตารางที่ 4. 29

ตารางแสดงค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่5 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. ความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญ	<1 ปี	19	3.6316	0.76089
	1-2 ปี	47	3.4043	0.57708
	3-4 ปี	25	3.2800	0.97980
	>4 ปี	19	3.6842	0.94591
	รวม	110	3.4636	0.78609
2. ความเหมาะสมของการควบคุมการเข้า-ออกบริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัย	<1 ปี	19	3.1579	0.76472
	1-2 ปี	47	3.4894	0.58504
	3-4 ปี	25	3.0800	01.03763
	>4 ปี	19	3.7895	0.63060
	รวม	110	3.3909	0.77927

ตารางที่ 4. 29 (ต่อ)

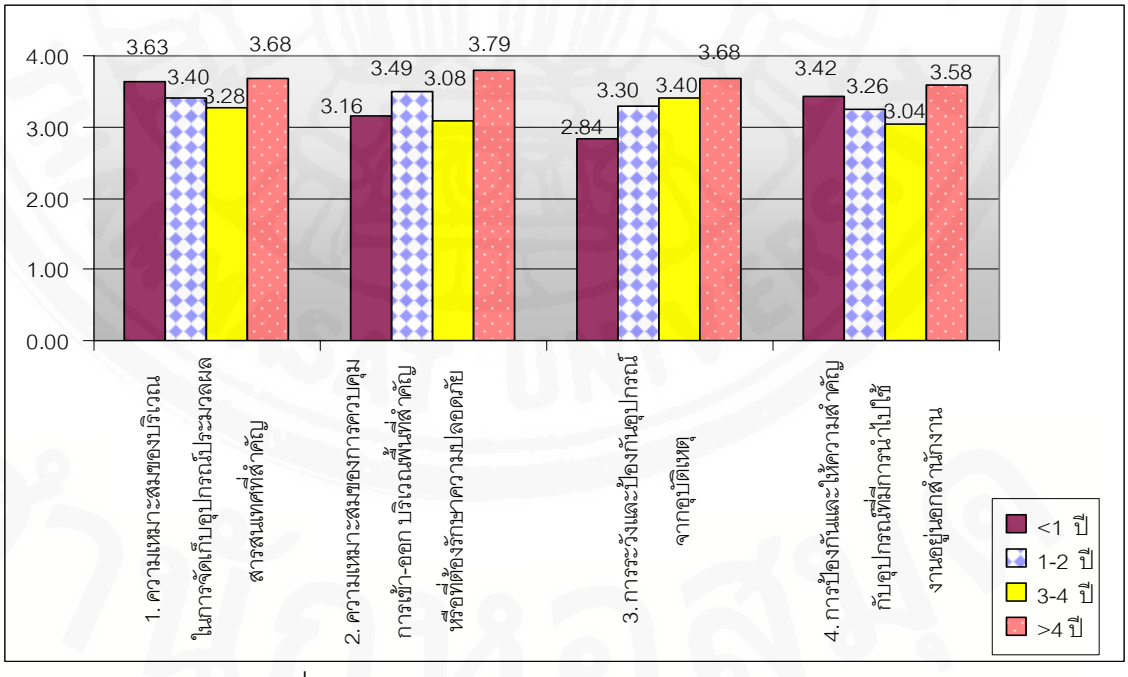
ตารางแสดงค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่5 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วง	จำนวน	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบน

	ระยะเวลา	(คน)		มาตรฐาน
3. การระวังและป้องกันอุปกรณ์จากอุบัติเหตุ	<1 ปี	19	2.8421	0.68825
	1-2 ปี	47	3.2979	0.80528
	3-4 ปี	25	3.4000	0.81650
	>4 ปี	19	3.6842	0.67104
	รวม	110	3.3091	0.79846
4. การป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงาน	<1 ปี	19	3.4211	0.50726
	1-2 ปี	47	3.2553	0.60678
	3-4 ปี	25	3.0400	0.97809
	>4 ปี	19	3.5789	0.60698
	รวม	110	3.2909	0.70834

ภาพที่ 4.29

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 5 แยกเป็นช่วงระยะเวลาการทำงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่ 5 จำแนกตามช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กร มีค่า 0.264 (Sig. = 0.264) มีค่ามากกว่าระดับนัยสำคัญ 0.05 ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กร มีค่า 0.008 (Sig. = 0.008) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงาน 3-4 ปี กับช่วงอายุงานที่มากกว่า 4 ปี

(3) ความคิดเห็นต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุ

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องการระวังและป้องกันอุปกรณ์จากอุบัติเหตุ มีค่า 0.010 (Sig. = 0.010) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆมีความคิดเห็นต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุแตกต่างกัน

โดยคู่ที่แตกต่างกันเรื่องความเหมาะสมของการต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงานต่ำกว่า 1 ปี กับช่วงอายุงานที่มากกว่า 4 ปี

(4) ความคิดเห็นต่อการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงาน มีค่า 0.0.69 (Sig. = 0.069) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า

ระยะอายุเวลาการทำงานต่างๆ มีความคิดเห็นต่อการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานไม่แตกต่างกัน

4.2.1.6 ผลสำรวจด้าน การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงาน เป็นดังตารางที่ 4.30 และภาพที่ 4.30

ตารางที่ 4. 30

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่6 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures)ตามระยะเวลาอันสมควร	<1 ปี	19	2.7368	0.65338
	1-2 ปี	47	3.1064	0.72932
	3-4 ปี	25	2.8400	0.74610
	>4 ปี	19	2.9474	0.77986
	รวม	110	2.9545	0.73430
2. ความเหมาะสมของการบริหารจัดการเครือข่าย (Network controls)และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application)ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย	<1 ปี	19	3.4737	0.69669
	1-2 ปี	47	3.5745	0.61661
	3-4 ปี	25	3.3200	0.80208
	>4 ปี	19	3.7895	0.53530
	รวม	110	3.5364	0.67290

ตารางที่ 4. 30 (ต่อ)

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่6 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
3. การจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่	<1 ปี	19	3.8947	0.73747

สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตหรือไม่เกี่ยวข้อง	1-2 ปี	47	3.5745	0.80067
	3-4 ปี	25	3.3600	0.90738
	>4 ปี	19	3.9474	0.62126
	รวม	110	3.6455	0.80806
4. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กร	<1 ปี	19	2.7895	0.91766
	1-2 ปี	47	3.2766	0.61510
	3-4 ปี	25	3.0000	0.76376
	>4 ปี	19	3.3684	0.76089
	รวม	110	3.1455	0.75220
5. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กร	<1 ปี	19	3.2632	0.87191
	1-2 ปี	47	3.2766	0.61510
	3-4 ปี	25	3.2400	0.59722
	>4 ปี	19	3.4737	0.61178
	รวม	110	3.3000	0.65735
6. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กร	<1 ปี	19	2.8421	0.68825
	1-2 ปี	47	3.4255	0.65091
	3-4 ปี	25	3.2000	0.57735
	>4 ปี	19	3.4211	0.60698
	รวม	110	3.2727	0.66234

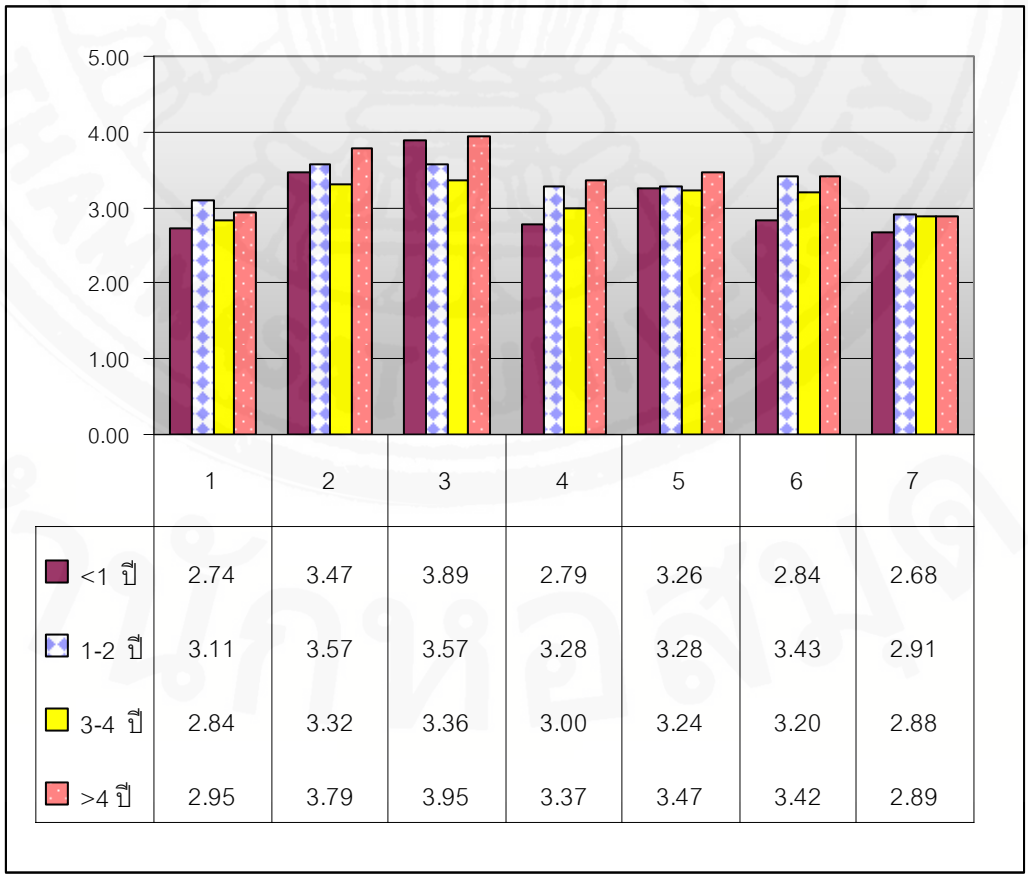
ตารางที่ 4. 30 (ต่อ)

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่6 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
7. การตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT	<1 ปี	19	2.6842	0.88523
	1-2 ปี	47	2.9149	0.82961
	3-4 ปี	25	2.8800	0.78102
	>4 ปี	19	2.8947	0.73747
	รวม	110	2.8636	0.80682

ภาพที่ 4. 30

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 6 แยกเป็นช่วงระยะเวลาการทำงาน



<u>หมายเหตุ</u> จากภาพที่ 4. 30 ตัวเลข 1-7 แทนมาตรฐานการรักษาความปลอดภัยดังนี้

1 = การปรับปรุงคู่มือ ตามระยะเวลาอันสมควร

2 = ความเหมาะสมของการบริหารจัดการเครือข่าย ระบบและโปรแกรมประยุกต์

3 = การจัดเก็บเอกสารข้อมูลต่างๆที่สำคัญ

4 = การทราบสิทธิของการส่งข้อมูลออกไปนอกองค์กร

5 = การทราบสิทธิของการใช้งานอินเตอร์เน็ตขององค์กร

6 = การทราบสิทธิของการใช้อีเมล์ขององค์กร

7 = การตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT

ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่6 จำแนกตามลักษณะหน่วยงานช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควร มีค่า 0.233 (Sig. = 0.233) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการปรับปรุงคู่มือขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควรไม่แตกต่างกัน

(2) ความคิดเห็นต่อความเหมาะสมของการบริหารจัดการเครือข่าย (Network controls) และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย มีค่า 0.132 (Sig. = 0.132) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่าระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายไม่แตกต่างกัน

(3) ความคิดเห็นต่อการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตหรือไม่เกี่ยวข้อง

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย มีค่า 0.045 (Sig. = 0.045) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตแตกต่างกันอย่างน้อย 1 คู่

แต่เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe กับไม่พบคู่ที่แตกต่างกัน

(4) ความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กร มีค่า 0.038 (Sig. = 0.038) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กรแตกต่างกันอย่างน้อย 1 คู่

แต่เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe กับไม่พบคู่ที่แตกต่างกัน

(5) ความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กร มีค่า 0.653 (Sig. = 0.653) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กรไม่แตกต่างกัน

(6) ความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กร มีค่า 0.007 (Sig. =0.007) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงานต่ำกว่า 1 ปีกับช่วงอายุงาน 1-2 ปี

(7) ความคิดเห็นต่อการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กร มีค่า 0.766 (Sig. = 0.766) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กรไม่แตกต่างกัน

4.2.1.7 ผลสำรวจด้าน การควบคุมการเข้าถึง (Access control)

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงาน เป็นดังตารางที่ 4.31 และภาพที่ 4.31

ตารางที่ 4. 31

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่7 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กร	<1 ปี	19	2.7895	0.63060
	1-2 ปี	47	3.3191	0.51526
	3-4 ปี	25	3.2000	0.64550
	>4 ปี	19	3.4737	0.77233
	รวม	110	3.2273	0.64480
2. การแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม(อาจทุก 3 เดือน หรือ 6 เดือน)	<1 ปี	19	3.6842	0.67104
	1-2 ปี	47	3.6596	0.81498
	3-4 ปี	25	3.4000	1.32288
	>4 ปี	19	3.4211	0.69248
	รวม	110	3.5636	0.91398

ตารางที่ 4. 31 (ต่อ)

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่7 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
3. การให้ความสำคัญกับการ Lock Off เครื่อง หรือปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน	<1 ปี	19	3.5789	0.96124
	1-2 ปี	47	2.9787	1.18852
	3-4 ปี	25	3.1600	1.28062
	>4 ปี	19	4.0000	1.15470
	รวม	110	3.3000	1.21572
4. การให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน	<1 ปี	19	3.7368	0.73349
	1-2 ปี	47	4.0213	0.67532
	3-4 ปี	25	3.5600	0.86987
	>4 ปี	19	4.3158	0.47757
	รวม	110	3.9182	0.74356
5. การให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กร	<1 ปี	19	3.7368	0.73349
	1-2 ปี	47	3.3404	0.70020
	3-4 ปี	25	3.4800	0.71414
	>4 ปี	19	3.9474	0.70504
	รวม	110	3.5455	0.73742
6. มาตรฐานระบบบริหารจัดการรหัสผ่าน (Password management system)	<1 ปี	19	3.2105	0.53530
	1-2 ปี	47	3.5957	0.79836
	3-4 ปี	25	3.2400	0.87939
	>4 ปี	19	3.8421	0.60214
	รวม	110	3.4909	0.77513
7. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์	<1 ปี	19	3.2632	0.73349
	1-2 ปี	47	3.1915	0.82458
	3-4 ปี	25	3.5600	0.86987

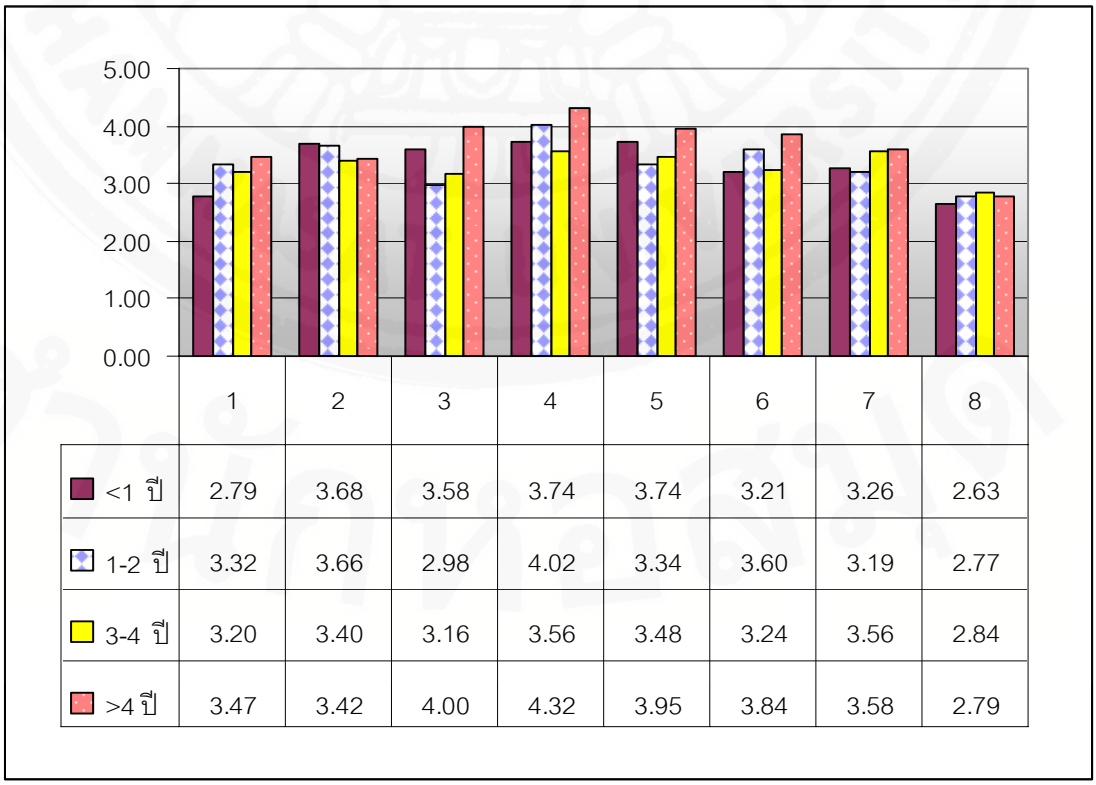
ตารางที่ 4. 31 (ต่อ)

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่7 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
7. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์	>4 ปี	19	3.5789	1.01739
	รวม	110	3.3545	0.86296
8. การตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร	<1 ปี	19	2.6316	0.95513
	1-2 ปี	47	2.7660	0.88986
	3-4 ปี	25	2.8400	0.85049
	>4 ปี	19	2.7895	0.78733
	รวม	110	2.7636	0.86658

ภาพที่ 4.31

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่7 แยกเป็นช่วงระยะเวลาการทำงาน



<u>หมายเหตุ</u> จากภาพที่ 4.31 ตัวเลข 1-8 แทนมาตรฐานการรักษาความปลอดภัยดังนี้

1 = การทราบสิทธิในการใช้งานระบบหรือโปรแกรมในองค์กร

2 = การแจ้งสิทธิของการใช้งานระบบและโปรแกรมให้ทราบตามระยะ

3 = การให้ความสำคัญกับการ Lock Off เครื่องหรือปิดเครื่อง

4 = การให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน

5 = การให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมขององค์กร

6 = มาตรฐานระบบบริหารจัดการรหัสผ่าน (Password management system)

7 = การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์

8 = การตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร

ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่7 จำแนกตามช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กร มีค่า 0.005 (Sig. = 0.005) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงานต่ำกว่า 1 ปีกับช่วงอายุงาน 1-2 ปี และ ช่วงอายุงานต่ำกว่า 1 ปีกับช่วงอายุงานมากกว่า 4 ปี

(2) ความคิดเห็นต่อการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม(อาจทุก 3 เดือน หรือ 6 เดือน)
สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) ไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) แตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) มีค่า 0.555 (Sig. = 0.555) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) ไม่แตกต่างกัน

(3) ความคิดเห็นต่อการให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน
สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานานไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานานแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน มีค่า 0.011 (Sig. = 0.011) ซึ่งมีค่าน้อยกว่าระดับ

นัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานานแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงาน 1-2 ปี กับ ช่วงอายุงานมากกว่า 4 ปี

(4) ความคิดเห็นต่อการให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งานไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งานแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง ให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน มีค่า 0.034 (Sig. = 034) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งานแตกต่างกัน อย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงาน 3-4 ปี กับ ช่วงอายุงานมากกว่า 4 ปี

(5) ความคิดเห็นต่อการให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กร มีค่า 0.011 (Sig. = 0.011) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงาน 1-2 ปี กับ ช่วงอายุงานมากกว่า 4 ปี

(6) ความคิดเห็นต่อมาตรฐานระบบบริหารจัดการรหัสผ่าน (Password management system) ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อมาตรฐานระบบบริหารจัดการรหัสผ่านขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อมาตรฐานระบบบริหารจัดการรหัสผ่านขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องมาตรฐานระบบบริหารจัดการรหัสผ่านขององค์กร มีค่า 0.018 (Sig. = 0.018) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ความคิดเห็นต่อมาตรฐานระบบบริหารจัดการรหัสผ่านขององค์กรแตกต่างกันอย่างน้อย 1 คู่

แต่เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe กับไม่พบคู่ที่แตกต่างกัน

(7) ความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆทราบกฎระเบียบข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์ไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีทราบกฎระเบียบข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์แตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์ มีค่า 0.205 (Sig. = 0.205) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์ไม่แตกต่างกัน

(8) ความคิดเห็นต่อการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ทำการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ทำการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร มีค่า 0.887 (Sig. = 0.887) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงสมมติฐานยอมรับ H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ทำการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรไม่แตกต่างกัน

4.2.1.8 ผลสำรวจด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงาน เป็นดังตารางที่ 4.32 และภาพที่ 4.32

ตารางที่ 4. 32

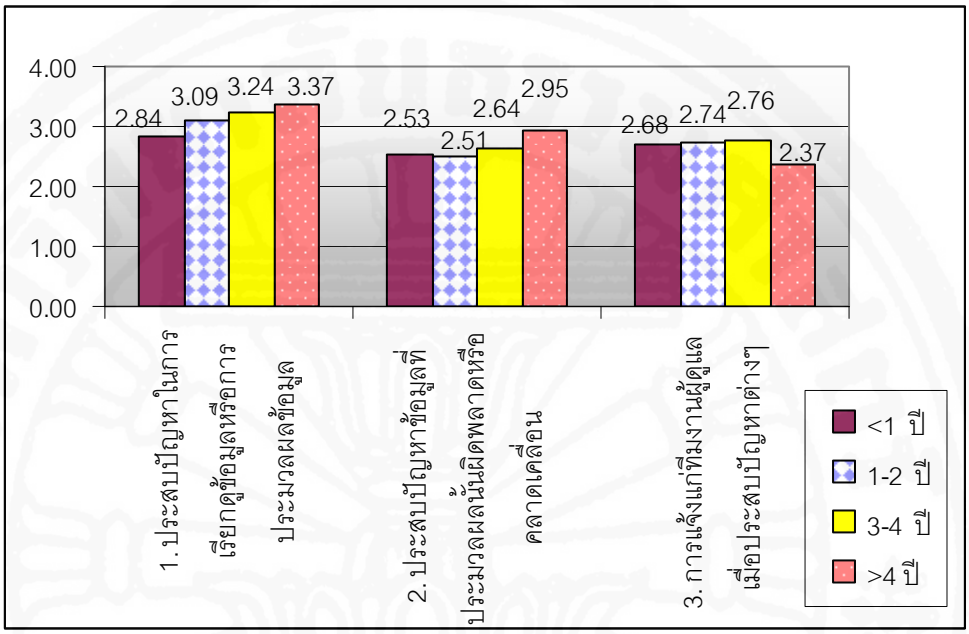
ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 8 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูล	<1 ปี	19	2.8421	0.83421
	1-2 ปี	47	3.0851	0.99629
	3-4 ปี	25	3.2400	1.09087
	>4 ปี	19	3.3684	0.83070
	รวม	110	3.1273	0.96839
2. ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อน	<1 ปี	19	2.5263	0.90483
	1-2 ปี	47	2.5106	0.74811
	3-4 ปี	25	2.6400	1.28712
	>4 ปี	19	2.9474	1.02598
	รวม	110	2.6182	0.96718
3. การแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆ	<1 ปี	19	2.6842	0.74927
	1-2 ปี	47	2.7447	0.67464
	3-4 ปี	25	2.7600	1.33167
	>4 ปี	19	2.3684	0.95513
	รวม	110	2.6727	0.91980

ภาพที่ 4. 32

แสดงกราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่8

แยกเป็นช่วงระยะเวลาการทำงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่8 จำแนกตามช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูล

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูล มีค่า 0.358 (Sig. = 0.358) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลไม่แตกต่างกัน

(2) ความคิดเห็นต่อการประสบปัญหาข้อมูลที่ประมวลผลผิดพลาดหรือคลาดเคลื่อน

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนมีค่า 0.401 (Sig. = 0.401) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนไม่แตกต่างกัน

(3) ความคิดเห็นต่อการแจ้งทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหา

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง ให้ความสำคัญกับการแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆ มีค่า 0.463 (Sig. = 0.463) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ แจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆ ไม่แตกต่างกัน

4.2.1.9 <u>ผลสำรวจด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงาน เป็นดังตารางที่ 4.33 และภาพที่ 4.33

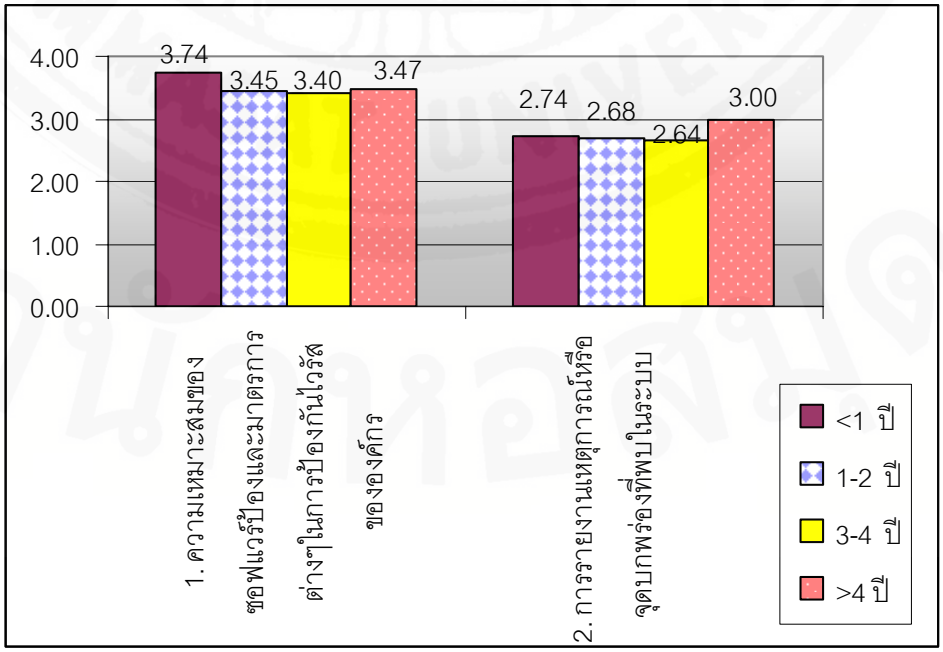
ตารางที่ 4.33

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่9 และส่วนเบี่ยงเบนมาตรฐาน แยกช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. ความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กร	<1 ปี	19	3.7368	0.65338
	1-2 ปี	47	3.4468	0.74625
	3-4 ปี	25	3.4000	0.81650
	>4 ปี	19	3.4737	0.77233
	รวม	110	3.4909	0.75109
2. การรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กร	<1 ปี	19	2.7368	0.99118
	1-2 ปี	47	2.6808	0.98038
	3-4 ปี	25	2.6400	1.28711
	>4 ปี	19	3.0000	0.81649
	รวม	110	2.7366	1.02873

ภาพที่ 4.33

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 9 แยกช่วงระยะเวลาการทำงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่ 9 จำแนกตามช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กร มีค่า 0.467 (Sig. = 0.467) ค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่าระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กร)

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กร ไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรมีค่า 0.664

(Sig. = 0.664) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่าระยะเวลาการทำงานต่างๆ มีการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กร ไม่แตกต่างกัน

4.2.1.10 ผลสำรวจด้าน การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

พบว่าค่าความคิดเห็นแบ่งแยกตามช่วงระยะเวลาการทำงาน เป็นดังตารางที่ 4.34 และภาพที่ 4.34

ตารางที่ 4.34

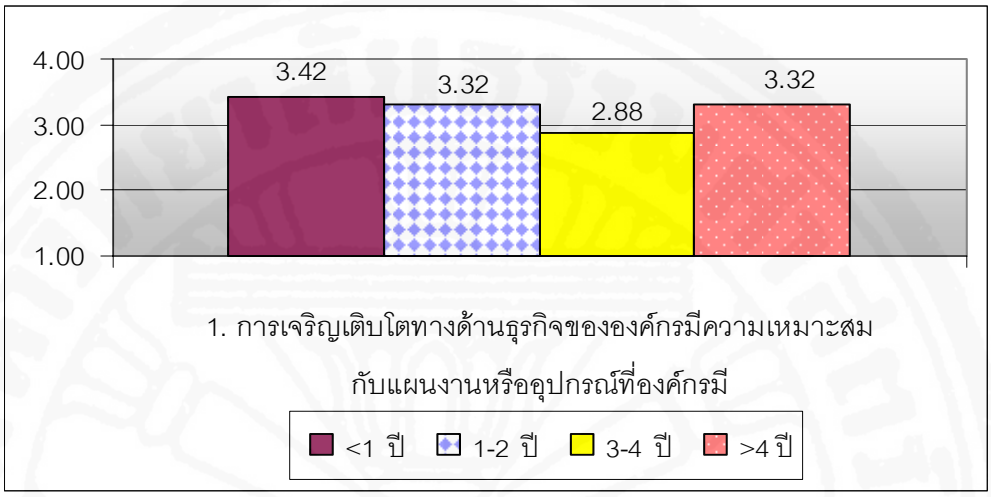
ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 10 และส่วนเบี่ยงเบนมาตรฐาน แยกช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมี	<1 ปี	19	3.4211	0.60698
	1-2 ปี	47	3.3191	0.72551
	3-4 ปี	25	2.8800	1.01325
	>4 ปี	19	3.3158	0.74927
	รวม	110	3.2364	0.80054

ภาพที่ 4.34

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่10

แยกเป็นช่วงระยะเวลาการทำงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่10 จำแนกตามช่วงระยะเวลาการทำงานทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมี

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมีไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมีแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมี มีค่า 0.082 (Sig. = 0.082) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมี ไม่แตกต่างกัน

4.2.1.11 ผลสำรวจด้าน การปฏิบัติตามข้อกำหนด (Compliance)

พบค่าความคิดเห็นตามช่วงระยะเวลาการทำงานเป็นดังตารางที่ 4.35และภาพที่ 4.35

ตารางที่ 4.35

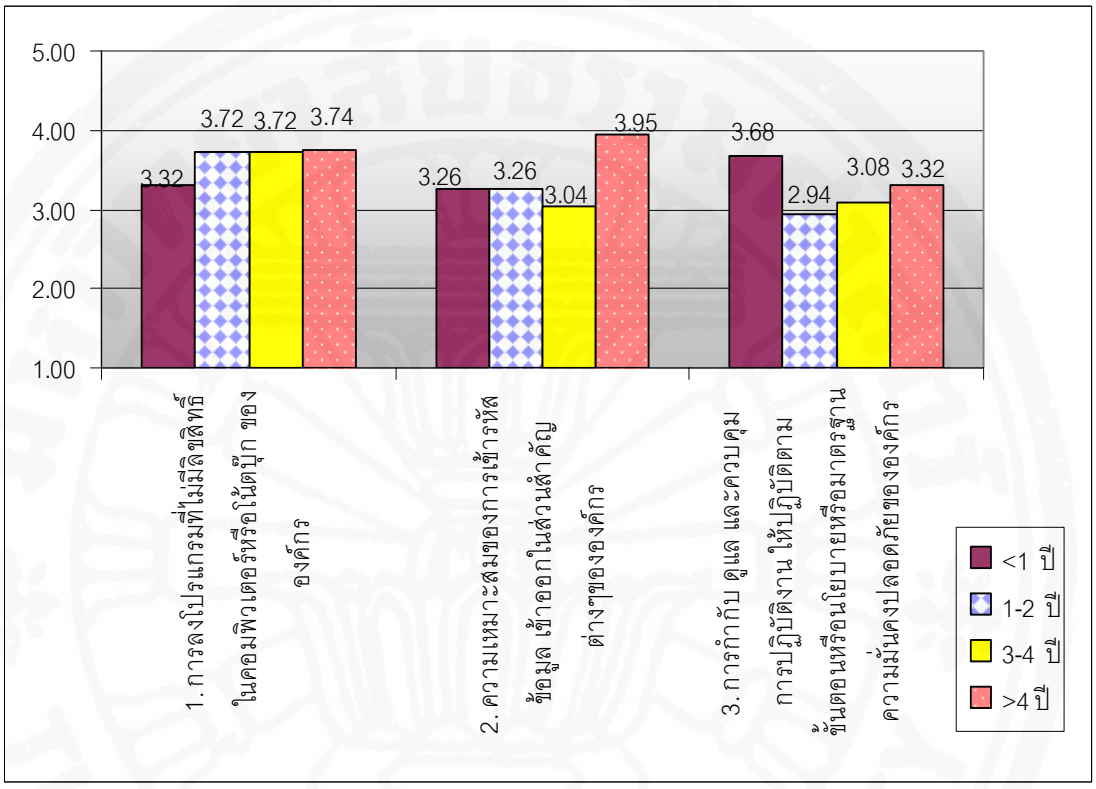
ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่11 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นช่วงระยะเวลาการทำงาน

มาตรฐานการรักษาความปลอดภัย	ช่วงระยะเวลา	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กร	<1 ปี	19	3.3158	2.02903
	1-2 ปี	47	3.7234	1.88475
	3-4 ปี	25	3.7200	1.90438
	>4 ปี	19	3.7368	1.91027
	รวม	110	3.6545	1.89851
2. ความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กร	<1 ปี	19	3.2632	0.45241
	1-2 ปี	47	3.2553	0.70612
	3-4 ปี	25	3.0400	0.61101
	>4 ปี	19	3.9474	0.52427
	รวม	110	3.3273	0.67876
3. การกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กร	<1 ปี	19	3.6842	0.74927
	1-2 ปี	47	2.9362	0.73438
	3-4 ปี	25	3.0800	0.75939
	>4 ปี	19	3.3158	0.88523
	รวม	110	3.1636	0.80739

ภาพที่ 4.35

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่11

แยกเป็นช่วงระยะเวลาการทำงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่ 11 จำแนกตามช่วงระยะเวลาการทำงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ผลสำรวจการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ทราบนโยบายการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ ทราบนโยบายการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการทราบทราบนโยบายการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กร มีค่า 0.869 (Sig. = 0.869) ค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน

H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ ทราบนโยบายการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กร มีค่า 0.000 (Sig. = 0.000) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ

- ช่วงอายุงานที่มากกว่า 4 ปีกับช่วงอายุงานที่ต่ำกว่า 1 ปี
- ช่วงอายุงานที่มากกว่า 4 ปีกับช่วงอายุงาน 1-2 ปี
- ช่วงอายุงานที่มากกว่า 4 ปีกับช่วงอายุงาน 3-4 ปี

(3) ความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{<1} = \mu_{1-2} = \mu_{3-4} = \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กรไม่แตกต่างกัน

H_1: $\mu_{<1} \neq \mu_{1-2} \neq \mu_{3-4} \neq \mu_{>4}$ ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง ความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กร มีค่า 0.005 (Sig. = 0.005) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า ระยะเวลาการทำงานต่างๆ มีความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กรแตกต่างกันอย่างน้อย 1 คู่

โดยคู่ที่แตกต่างกันเรื่องความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กร เมื่อดูจากตาราง Multiple Comparisons ของ Scheffe คือ ช่วงอายุงาน 1-2 ปีกับช่วงอายุงานที่ต่ำกว่า 1 ปี

4.2.2 <u>สมมติฐานข้อที่ 2</u>

หน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ(IT) กับหน่วยงานที่ไม่เกี่ยวข้องกับระบบสารสนเทศ (IT) มีความคิดเห็นต่อเรื่อง ความปลอดภัยด้านระบบสารสนเทศไม่แตกต่างกัน จากการทดสอบทางสถิติด้วยวิธี T-Test โดยแยกเป็นรายข้อตามมาตรฐาน ISO 17799 จำนวน 11 ข้อใหญ่ เป็นดังนี้

4.2.2.1 <u>ผลสำรวจด้าน นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.36 และภาพที่ 4.36

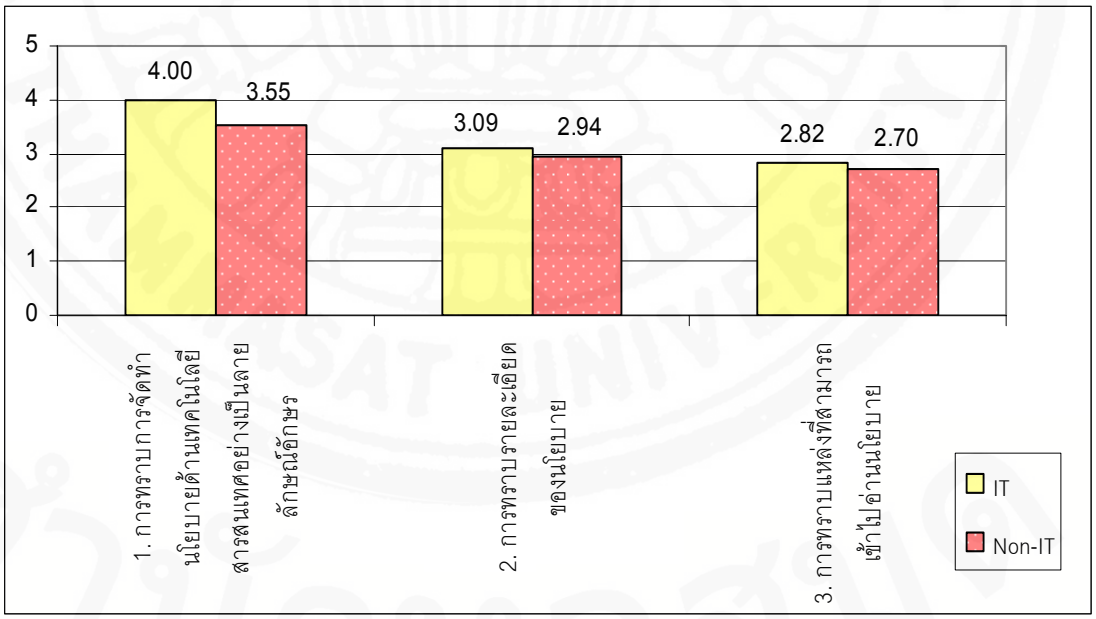
ตารางที่ 4.36

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่1และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร	IT	44	4.0000	1.75208
	Non-IT	66	3.5455	1.93893
2. การทราบรายละเอียดของนโยบาย	IT	44	3.0909	2.02103
	Non-IT	66	2.9394	2.01440
3. การทราบแหล่งที่สามารถเข้าไปอ่านนโยบาย	IT	44	2.8182	2.01474
	Non-IT	66	2.6970	1.99206

ภาพที่ 4.36

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่1 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่1 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กร มีค่า 0.205 (Sig. = 0.205) ซึ่งมากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบการจัดทำนโยบายด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษรขององค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อการทราบรายละเอียดของนโยบายขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบรายละเอียดของนโยบายขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบรายละเอียดของนโยบายขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบรายละเอียดของนโยบายขององค์กร มีค่า 0.700 (Sig. = 0.700) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบรายละเอียดของนโยบายขององค์กรไม่แตกต่างกัน

(3) ความคิดเห็นต่อการรทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กร มีค่า 0.756 (Sig. = 0.756) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบแหล่งที่สามารถเข้าไปอ่านนโยบายขององค์กรไม่แตกต่างกัน

4.2.2.2 <u>โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization) และที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.37และภาพที่ 4.37

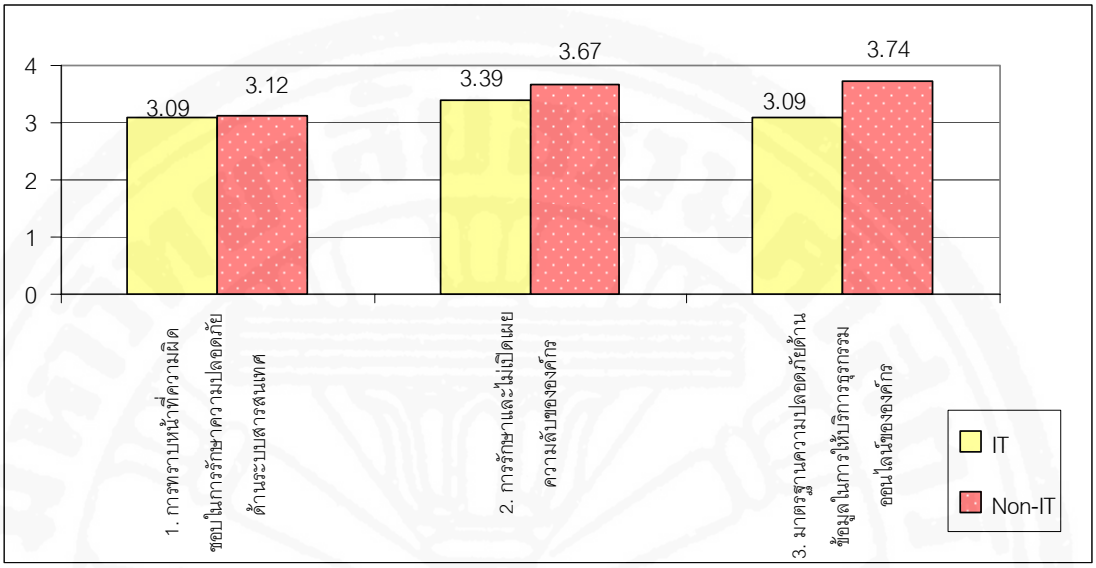
ตารางที่4. 37

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่2 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศ	IT	44	3.0909	0.85775
	Non-IT	66	3.1212	0.92012
2. การรักษาและไม่เปิดเผยความลับขององค์กร	IT	44	3.3864	1.10424
	Non-IT	66	3.6667	0.88289
3. มาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กร	IT	44	3.0909	0.60302
	Non-IT	66	3.7424	0.82854

ภาพที่ 4.37

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่2 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่2 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ความคิดเห็นต่อการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กร มีค่า 0.862 (Sig. = 0.862) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่าหน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบหน้าที่ความผิดชอบในการรักษาความปลอดภัยด้านระบบสารสนเทศต่อองค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อการรักษาและไม่เปิดเผยความลับขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการรักษาและไม่เปิดเผยความลับขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการรักษาและไม่เปิดเผยความลับขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการรักษาและไม่เปิดเผยความลับขององค์กร มีค่า 0.143 (Sig. = 0.143) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการรักษาและไม่เปิดเผยความลับขององค์กรไม่แตกต่างกัน

(3) ความคิดเห็นต่อมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กร

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กร มีค่า 0.000 (Sig. = 0.000) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อมาตรฐานความปลอดภัยด้านข้อมูลในการให้บริการธุรกรรมออนไลน์ขององค์กรแตกต่างกัน

4.2.2.3 <u>ผลสำรวจด้าน หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) และการจัดหมวดหมู่สารสนเทศ (Information classification)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.38และภาพที่ 4.38

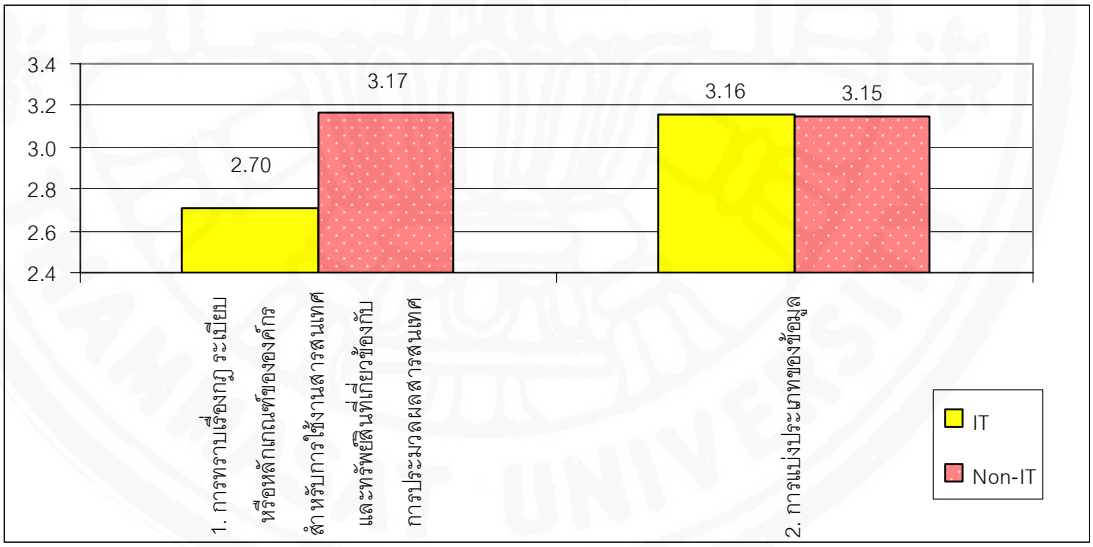
ตารางที่ 4.38

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่3และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ	IT	44	2.7045	0.79474
	Non-IT	66	3.1667	0.66986
2. การแบ่งประเภทของข้อมูล	IT	44	3.1591	0.77589
	Non-IT	66	3.1515	0.74920

ภาพที่ 4.38

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 3 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่3 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการทราบกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ มีค่า 0.002 (Sig. = 0.002) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศแตกต่างกัน

(2) ความคิดเห็นต่อการแบ่งประเภทของข้อมูล

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการแบ่งประเภทของข้อมูลไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการแบ่งประเภทของข้อมูลแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องการความคิดเห็นต่อการแบ่งประเภทของข้อมูล มีค่า 0.959 (Sig. = 0.959) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการแบ่งประเภทของข้อมูลไม่แตกต่างกัน

4.2.2.4 ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment) และในระหว่างการจ้างงาน (During employment)

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.39 และภาพที่ 4.39

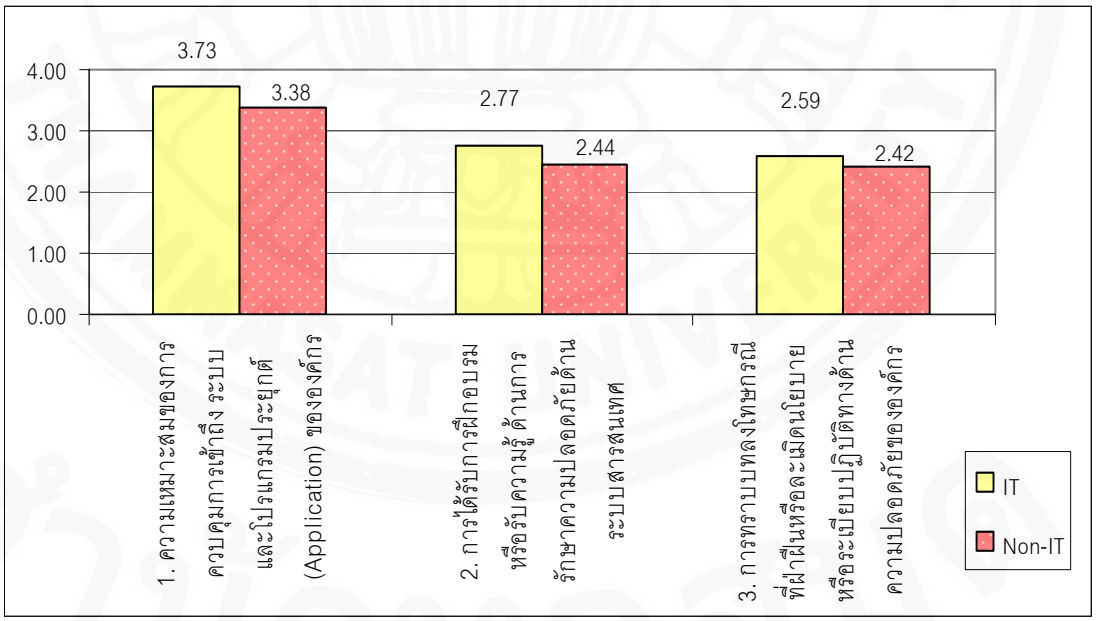
ตารางที่ 4.39

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่4 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. ความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์(Application) ขององค์กร	IT	44	3.7273	0.65994
	Non-IT	66	3.3788	0.71823
2. การได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศ	IT	44	2.7727	0.80301
	Non-IT	66	2.4394	0.91364
3. การทราบบทลงโทษกรณีฝ่าฝืนหรือละเมิดนโยบายระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กร	IT	44	2.5909	0.78705
	Non-IT	66	2.4242	0.92919

ภาพที่ 4.39

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่4 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่4 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์(Application) ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์ (Application) ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์ (Application) ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานเรื่องความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์ (Application) ขององค์กร มีค่า 0.011 (Sig. = 0.011) มีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้าถึง ระบบและโปรแกรมประยุกต์ (Application) ขององค์กรแตกต่างกัน

(2) ความคิดเห็นต่อการได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศ

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการได้รับการฝึกอบรมหรือรับความรู้ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศ มีค่า 0.052 (Sig. = 0.052) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศไม่แตกต่างกัน

(3) ความคิดเห็นต่อการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กร

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กร มีค่า 0.330 (Sig. = 0.330) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบบทลงโทษกรณีที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กรไม่แตกต่างกัน

4.2.2.5 <u>ผลสำรวจด้าน การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.40 และภาพที่ 4.40

ตารางที่ 4.40

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 5 และส่วนเบี่ยงเบนมาตรฐานแยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. ความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญ	IT	44	3.5000	0.73136
	Non-IT	66	3.4394	0.82516
2. ความเหมาะสมของการควบคุมการเข้า-ออกบริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัย	IT	44	3.3636	0.74991
	Non-IT	66	3.4091	0.80340

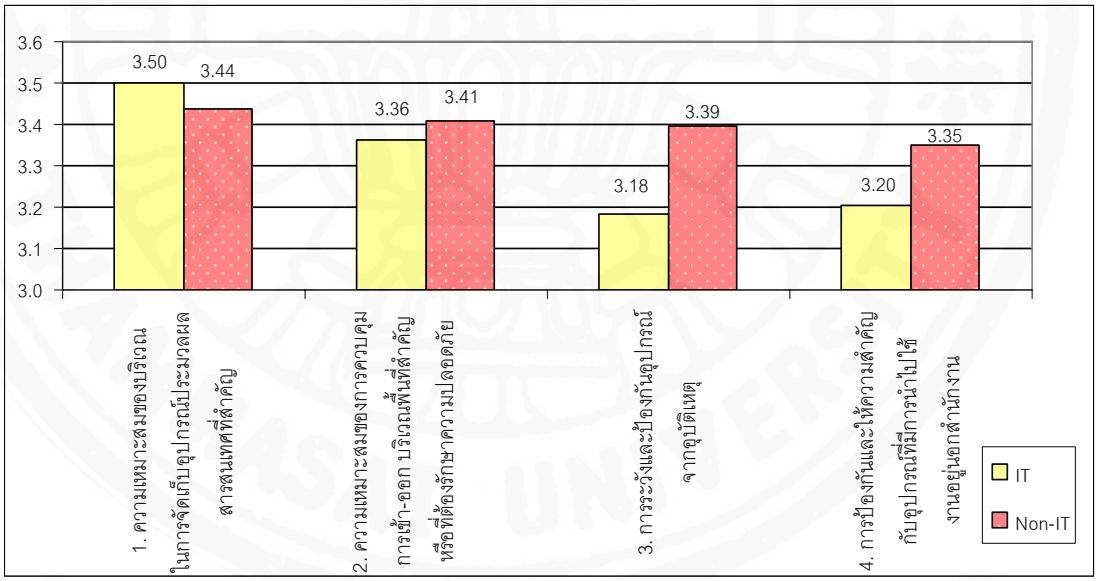
ตารางที่ 4.40 (ต่อ)

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 5 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
3. การระวังและป้องกันอุปกรณ์จากอุบัติเหตุ	IT	44	3.1818	0.89632
	Non-IT	66	3.3939	0.72066
4. การป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงาน	IT	44	3.2045	0.79474
	Non-IT	66	3.3485	0.64432

ภาพที่ 4.40

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 5 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่5 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กร มีค่า 0.694 (Sig. = 0.694) มีค่ามากกว่าระดับนัยสำคัญ 0.05 ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของบริเวณในการจัดเก็บอุปกรณ์ประมวลผลสารสนเทศที่สำคัญขององค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กร มีค่า 0.766 (Sig. = 0.766) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการควบคุมการเข้า-ออก บริเวณพื้นที่สำคัญหรือที่ต้องรักษาความปลอดภัยขององค์กรไม่แตกต่างกัน

(3) ความคิดเห็นต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุ

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องการระวังและป้องกันอุปกรณ์จากอุบัติเหตุ มีค่า 0.193 (Sig. = 0.193) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการระวังและป้องกันอุปกรณ์จากอุบัติเหตุไม่แตกต่างกัน

(4) ความคิดเห็นต่อการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานภัยความปลอดภัยเรื่องการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงาน มีค่า 0.299 (Sig. = 0.299) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการป้องกันและให้ความสำคัญกับอุปกรณ์ที่มีการนำไปใช้งานอยู่นอกสำนักงานไม่แตกต่างกัน

4.2.2.6 <u>ผลสำรวจด้าน การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.41 และภาพที่ 4.41

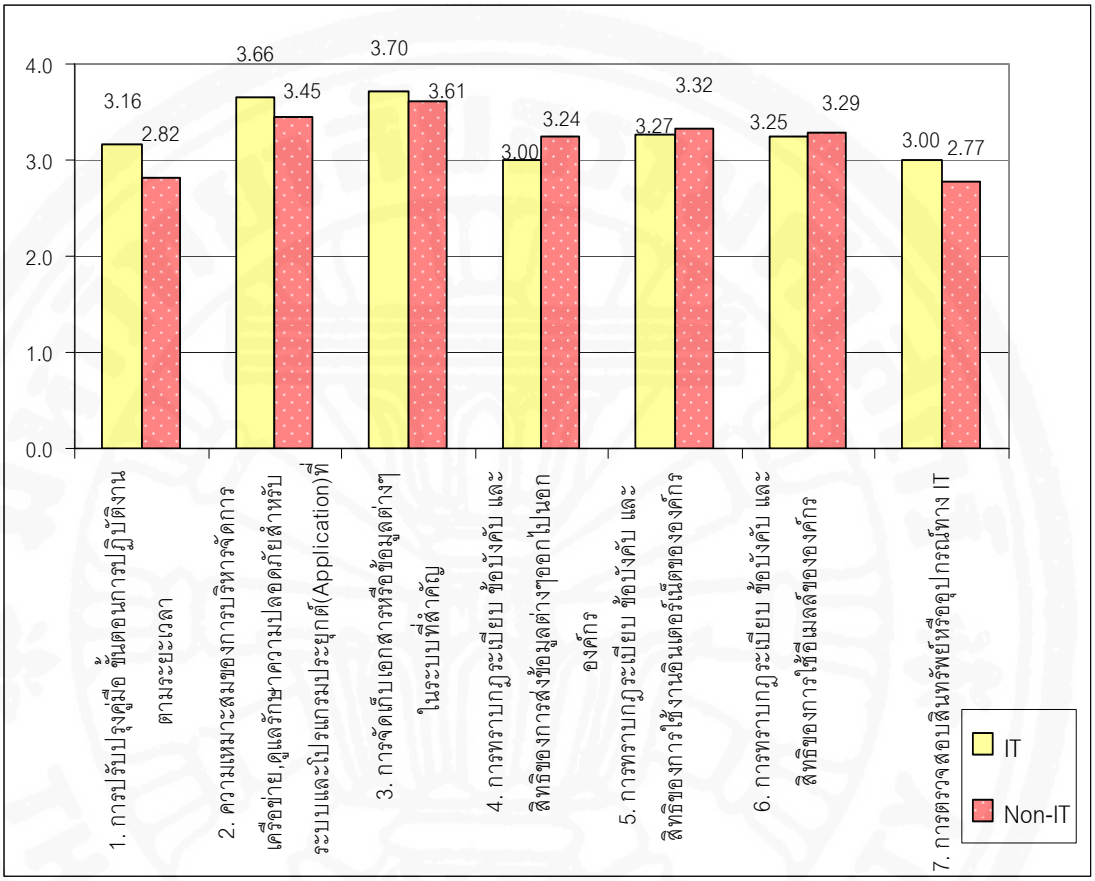
ตารางที่4. 41

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่6 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures)ตามระยะเวลาอันสมควร	IT	44	3.1591	0.64495
	Non-IT	66	2.8182	0.76277
2. ความเหมาะสมของการบริหารจัดการเครือข่าย (Network controls)และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application)ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย	IT	44	3.6591	0.56828
	Non-IT	66	3.4545	0.72710
3. การจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตหรือไม่เกี่ยวข้อง	IT	44	3.7045	0.87815
	Non-IT	66	3.6061	0.76216
4. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กร	IT	44	3.0000	0.60999
	Non-IT	66	3.2424	0.82389
5. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กร	IT	44	3.2727	0.62370
	Non-IT	66	3.3182	0.68296
6. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กร	IT	44	3.2500	0.61474
	Non-IT	66	3.2879	0.69648
7. การตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT	IT	44	3.0000	0.57060
	Non-IT	66	2.7727	0.92479

ภาพที่ 4.41

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่6 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่6 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควร มีค่า 0.016 (Sig. = 0.016) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures) ตามระยะเวลาอันสมควรแตกต่างกัน

(2) ความคิดเห็นต่อความเหมาะสมของการบริหารจัดการเครือข่าย (Network controls) และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย มีค่า 0.119 (Sig. = 0.119) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่ายไม่แตกต่างกัน

(3) ความคิดเห็นต่อการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตหรือไม่เกี่ยวข้อง

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการบริหารจัดการเครือข่าย, การดูแลรักษาความปลอดภัยสำหรับระบบและโปรแกรมประยุกต์ (Application) ที่ใช้งานในเครือข่าย รวมทั้งข้อมูลต่างๆ ที่ส่งผ่านทางเครือข่าย มีค่า 0.534 (Sig. = 0.534) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการจัดเก็บเอกสารหรือข้อมูลต่างๆในระบบที่สำคัญ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตไม่แตกต่างกัน

(4) ความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กร มีค่า 0.079 (Sig. = 0. 0.079) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการส่งข้อมูลต่างๆออกไปนอกองค์กรไม่แตกต่างกัน

(5) ความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กร มีค่า 0.724 (Sig. = 0.724) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้งานอินเตอร์เน็ตขององค์กรไม่แตกต่างกัน

(6) ความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมลล์ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กร มีค่า 0.770 (Sig. = 0.770) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน IT และหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการใช้อีเมล์ขององค์กรไม่แตกต่างกัน

(7) ความคิดเห็นต่อการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กร มีค่า 0.114 (Sig. = 0.114) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการตรวจสอบสินทรัพย์หรืออุปกรณ์ทาง IT ขององค์กรไม่แตกต่างกัน

4.2.2.7 <u>ผลสำรวจด้าน การควบคุมการเข้าถึง (Access control)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.42 และภาพที่ 4.42

ตารางที่ 4.42

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่7 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กร	IT	44	3.3636	0.68509
	Non-IT	66	3.1364	0.60476
2. การแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม(อาจทุก 3 เดือน หรือ 6 เดือน)	IT	44	3.2273	0.96119
	Non-IT	66	3.7879	0.81364
3. การให้ความสำคัญกับการ Lock Off เครื่อง หรือปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน	IT	44	3.7727	0.98509
	Non-IT	66	2.9848	1.25872
4. การให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน	IT	44	3.6364	0.74991
	Non-IT	66	4.1061	0.68228
5. การให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กร	IT	44	3.4773	0.73100
	Non-IT	66	3.5909	0.74374

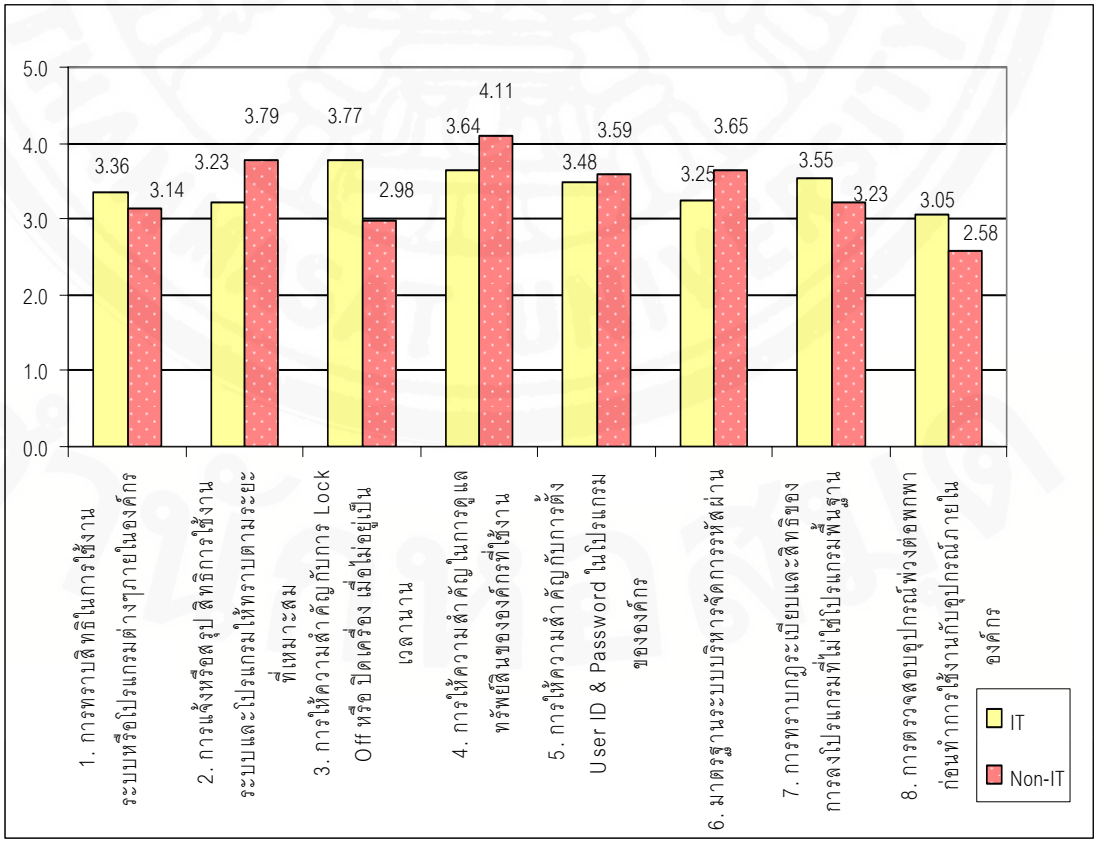
ตารางที่ 4.42 (ต่อ)

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่7 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
6. มาตรฐานระบบบริหารจัดการรหัสผ่าน (Password management system)	IT	44	3.2500	0.83874
	Non-IT	66	3.6515	0.69043
7. การทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์	IT	44	3.5455	0.58883
	Non-IT	66	3.2273	0.98910
8. การตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร	IT	44	3.0455	0.77623
	Non-IT	66	2.5758	0.87812

ภาพที่ 4.42

แสดงกราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่ 7 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่7 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT การทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กร มีค่า 0.078 (Sig. = 0.078) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน IT และหน่วยงานที่ไม่ใช่ IT การทราบสิทธิในการใช้งานระบบหรือโปรแกรมต่างๆภายในองค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม(อาจทุก 3 เดือน หรือ 6 เดือน)

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) ไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) แตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) มีค่า 0.001 (Sig. = 0.001) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่

IT มีความคิดเห็นต่อการแจ้ง หรือสรุป สิทธิของการใช้งานระบบและโปรแกรมต่างๆภายในองค์กร ให้ทราบตามระยะเวลาที่เหมาะสม (อาจทุก 3 เดือน หรือ 6 เดือน) แตกต่างกัน

(3) ความคิดเห็นต่อการให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานานไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานานแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน มีค่า 0.000 (Sig. = 0.000) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานานแตกต่างกัน

(4) ความคิดเห็นต่อการให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งานไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งานแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง ให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งาน มีค่า 0.001 (Sig. = 001) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญในการดูแลทรัพย์สินขององค์กรที่ใช้งานแตกต่างกัน

(5) ความคิดเห็นต่อการให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กร มีค่า 0.431 (Sig. = 0.431) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ให้ความสำคัญกับการตั้ง User ID & Password ในโปรแกรมต่างๆขององค์กรไม่แตกต่างกัน

(6) ความคิดเห็นต่อมาตรฐานระบบบริหารจัดการรหัสผ่าน (Password management system) ขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ความคิดเห็นต่อมาตรฐานระบบบริหารจัดการรหัสผ่านขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ความคิดเห็นต่อมาตรฐานระบบบริหารจัดการรหัสผ่านขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องมาตรฐานระบบบริหารจัดการรหัสผ่านขององค์กร มีค่า 0.007 (Sig. = 0.007) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับปฏิเสธสมมติฐาน H_0 และสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ความคิดเห็นต่อมาตรฐานระบบบริหารจัดการรหัสผ่านขององค์กรแตกต่างกัน

(7) ความคิดเห็นต่อการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทราบกฎระเบียบข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์ไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์แตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์ มีค่า 0.037 (Sig. = 0.037) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทราบกฎระเบียบ ข้อบังคับ และสิทธิของการลงโปรแกรมเฉพาะต่างๆขององค์กร หรือโปรแกรมอื่นๆที่ไม่ใช่โปรแกรมพื้นฐานของเครื่องคอมพิวเตอร์แตกต่างกัน

(8) ความคิดเห็นต่อการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทำการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทำการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร มีค่า 0.004 (Sig. = 0.004) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทำการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรแตกต่างกัน

4.2.2.8 ผลสำรวจด้าน การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.43 และภาพที่ 4.43

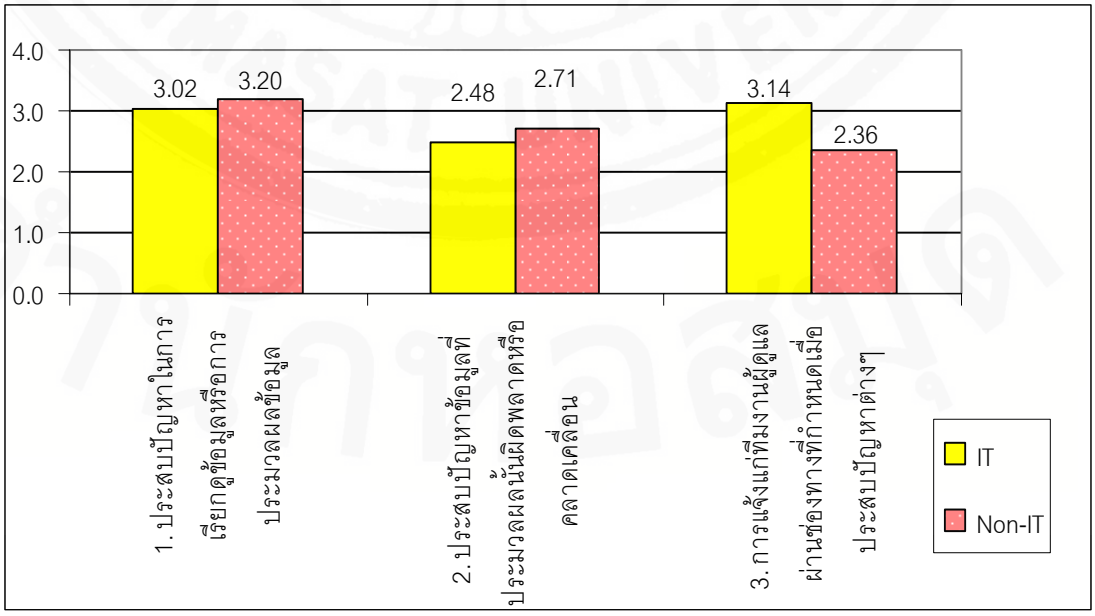
ตารางที่4.43

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่8 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูล	IT	44	3.0227	0.92733
	Non-IT	66	3.1970	0.99568
2. ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อน	IT	44	2.4773	0.73100
	Non-IT	66	2.7121	1.09214
3. การแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆ	IT	44	3.1364	0.66790
	Non-IT	66	2.3636	0.93868

ภาพที่ 4.43

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่8 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่8 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูล

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูล มีค่า 0.358 (Sig. = 0.358) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ประสบปัญหาในการเรียกดูข้อมูลหรือการประมวลผลข้อมูลไม่แตกต่างกัน

(2) ความคิดเห็นต่อการประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อน

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนมีค่า 0.180 (Sig. = 0.180) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน IT และหน่วยงานที่ไม่ใช่ IT ประสบปัญหาข้อมูลที่ประมวลผลนั้นผิดพลาดหรือคลาดเคลื่อนไม่แตกต่างกัน

(3) ความคิดเห็นต่อการแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆ

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT แจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT แจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง ให้ความสำคัญกับการแจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆ มีค่า 0.000 (Sig. = 0.000) ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงปฏิเสธสมมติฐาน H_0 และยอมรับสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT แจ้งแก่ทีมงานผู้ดูแลผ่านช่องทางที่กำหนดเมื่อประสบปัญหาต่างๆแตกต่างกัน

4.2.2.9 <u>ผลสำรวจด้าน การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.44 และภาพที่ 4.44

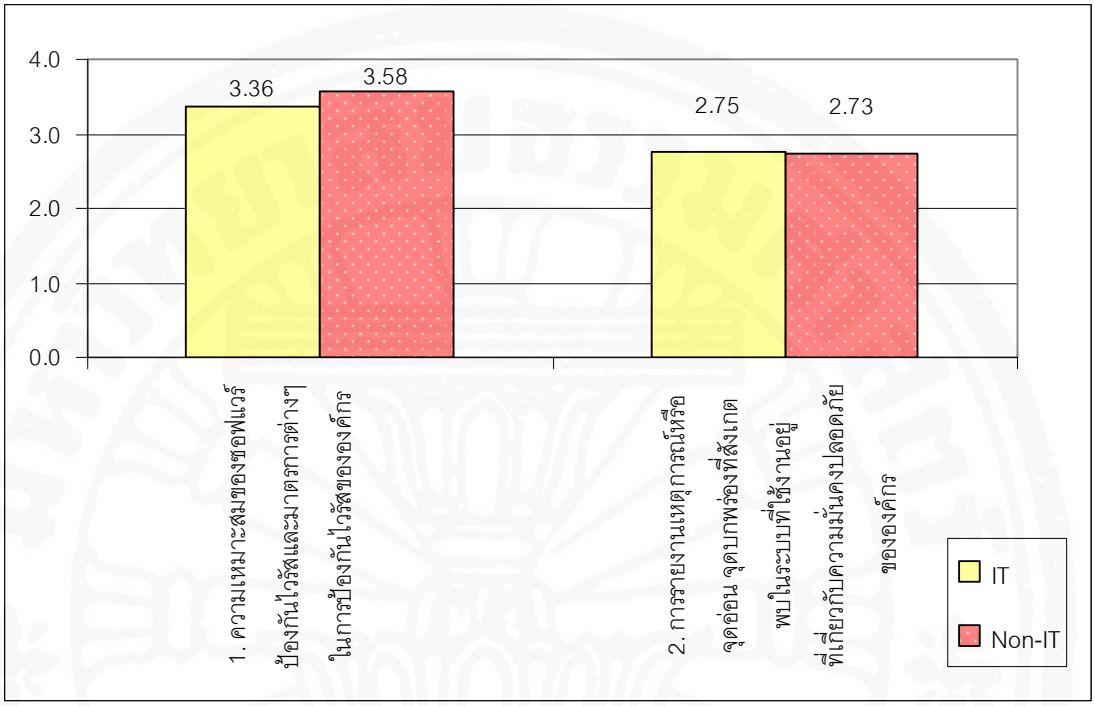
ตารางที่4.44

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่9 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. ความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กร	IT	44	3.3636	0.65026
	Non-IT	66	3.5758	0.80500
2. การรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กร	IT	44	2.75000	0.991241
	Non-IT	66	2.72727	1.060413

ภาพที่ 4.44

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่9 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่9 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non-IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non-IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กร มีค่า 0.148 (Sig. =

0.148) ค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่าหน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ความคิดเห็นต่อความเหมาะสมของซอฟแวร์ป้องกันไวรัสและมาตรการต่างๆในการป้องกันไวรัสขององค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กร)

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรมีค่า 0.910 (Sig. = 0.910) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่าหน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีการรายงานเหตุการณ์หรือจุดอ่อน จุดบกพร่องที่สังเกตพบในระบบที่ใช้งานอยู่ที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กร ไม่แตกต่างกัน

4.2.2.10 <u>ผลสำรวจด้าน การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.45 และภาพที่ 4.45

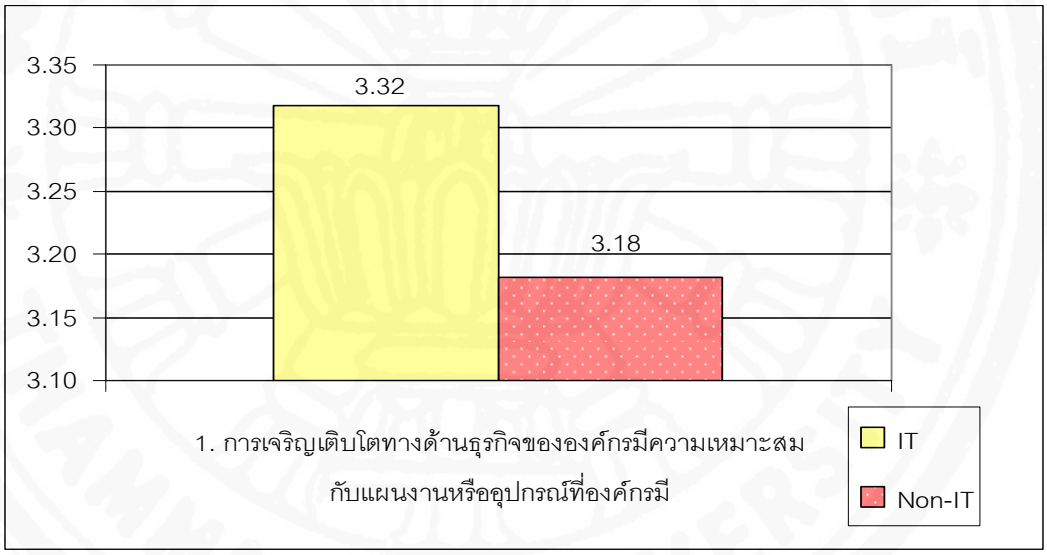
ตารางที่4. 45

ค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่10 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมี	IT	44	3.3182	0.85651
	Non-IT	66	3.1818	0.76277

ภาพที่ 4.45

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่10 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่10 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ความคิดเห็นต่อการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมี

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมีไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมีแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมี มีค่า 0.395 (Sig. = 0.395) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการเจริญเติบโตทางด้านธุรกิจขององค์กรมีความเหมาะสมกับแผนงานหรืออุปกรณ์ที่องค์กรมีไม่แตกต่างกัน

4.2.2.11 <u>ผลสำรวจด้าน การปฏิบัติตามข้อกำหนด (Compliance)</u>

พบว่าค่าความคิดเห็นแบ่งแยกตามหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ (IT) เป็นดังตารางที่ 4.46 และภาพที่ 4.46

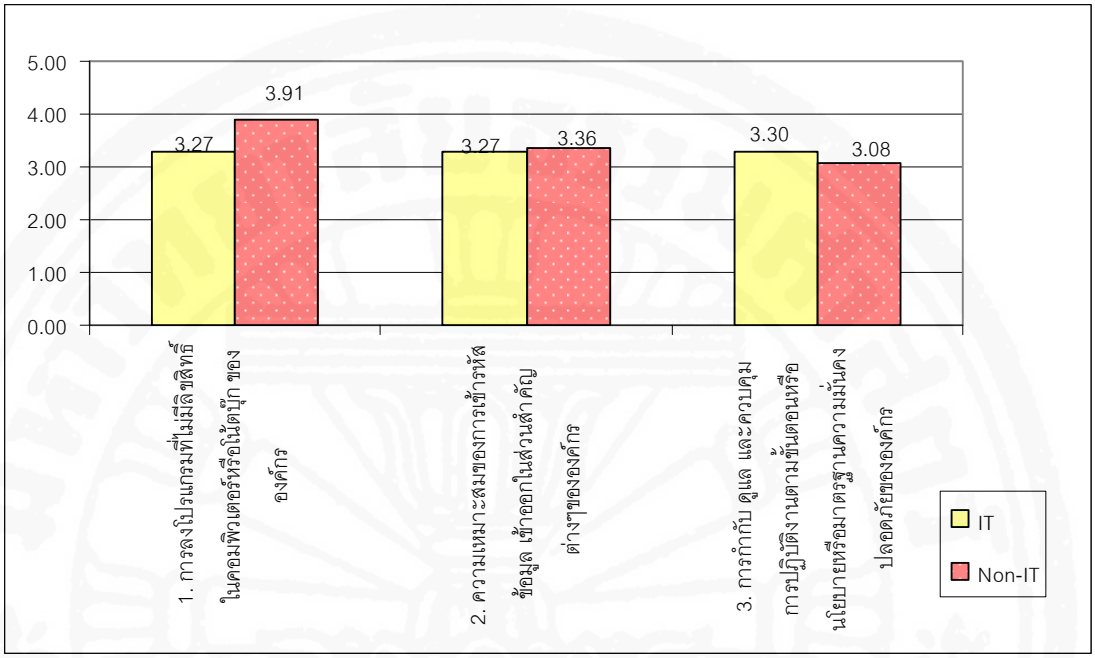
ตารางที่4.46

ตารางแสดงค่าเฉลี่ยมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่11 และส่วนเบี่ยงเบนมาตรฐาน แยกเป็นหน่วยงาน

มาตรฐานการรักษาความปลอดภัย	หน่วยงาน	จำนวน (คน)	ค่าเฉลี่ย	ค่าส่วนเบี่ยงเบนมาตรฐาน
1. การลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กร	IT	44	3.2727	2.00422
	Non-IT	66	3.9091	1.79510
2. ความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กร	IT	44	3.2727	0.72701
	Non-IT	66	3.3636	0.64775
3. การกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กร	IT	44	3.2955	0.66750
	Non-IT	66	3.0758	0.88249

ภาพที่ 4.46

กราฟมาตรฐานการรักษาความปลอดภัย ISO17799 ตามข้อที่11 แยกเป็นหน่วยงาน



ความคิดเห็นเรื่องมาตรฐานในการรักษาความปลอดภัยของข้อมูล ISO17799 ตามข้อที่11 จำแนกตามลักษณะหน่วยงาน ทำการทดสอบที่ระดับความเชื่อมั่น 95% หรือที่ระดับนัยสำคัญ 0.05 (α = 0.05)

(1) ผลสำรวจการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กร สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทราบนโยบายการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทราบนโยบายการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องการทราบทราบนโยบายการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กร มีค่า 0.093 (Sig. = 0.093) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ทราบนโยบายการลงโปรแกรมที่ไม่มีลิขสิทธิ์ในคอมพิวเตอร์หรือโน้ตบุ๊ก ขององค์กรไม่แตกต่างกัน

(2) ความคิดเห็นต่อความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กร

สมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กรไม่แตกต่างกัน

H1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่องความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กร มีค่า 0.494 (Sig. = 0.494) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อความเหมาะสมของการเข้ารหัสข้อมูล เข้าออกในส่วนสำคัญต่างๆขององค์กรไม่แตกต่างกัน

(3) ความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กรสมมติฐานทางสถิติ

H_0: $\mu_{IT} = \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กรไม่แตกต่างกัน

H_1: $\mu_{IT} \neq \mu_{Non\text{-}IT}$ หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT ความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กรแตกต่างกัน

ค่า Sig. สำหรับมาตรฐานความปลอดภัยเรื่อง ให้ความสำคัญกับการ Lock Off เครื่อง หรือ ปิดเครื่อง เมื่อไม่อยู่เป็นเวลานาน มีค่า 0.163 (Sig. = 0.163) ซึ่งมีค่ามากกว่าระดับนัยสำคัญ 0.05 (α = 0.05) ดังนั้นจึงยอมรับสมมติฐาน H_0 และปฏิเสธสมมติฐาน H_1 สรุปได้ว่า หน่วยงานด้าน ITและหน่วยงานที่ไม่ใช่ IT มีความคิดเห็นต่อการที่ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงาน ให้ปฏิบัติตามขั้นตอนหรือนโยบายหรือมาตรฐานความมั่นคงปลอดภัยขององค์กรไม่แตกต่างกัน

4.3 การวิเคราะห์ความเสี่ยง

การที่องค์กรต้องมีการประเมินความเสี่ยง เนื่องจากความจำเป็นที่องค์กรต้องสร้างความมั่นคงปลอดภัย ทั้งในแง่ของความถูกต้อง ความลับของข้อมูล และความพร้อมสำหรับการใช้งานข้อมูลและสารสนเทศ จึงจำเป็นที่องค์กรควรมีการประเมินความเสี่ยงที่อาจเกิดขึ้นได้ เพื่อจะได้เตรียมความพร้อม สำหรับกำหนดแนวทางในการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นเหล่านั้น

โดยหลังจากการสำรวจและการประเมินความเสี่ยงจากพนักงานในองค์กรที่เกี่ยวข้องมาแล้วนั้น มีทั้งหมด 7 เหตุการณ์ที่จัดเป็นความเสี่ยงสูงขององค์กรตัวอย่าง ที่องค์กรควรให้ความสนใจก่อน โดยเรียงตามลำดับความเสี่ยงจากมากไปน้อย ดังนี้

1. การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด
2. การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้
3. การใช้ชื่อ (User ID)ร่วมกันเพื่อเข้าใช้ข้อมูล
4. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม
5. ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้
6. Router / Firewall เสียทำให้ไม่สามารถใช้งานได้
7. ฐานข้อมูล(database)ถูกขัดจังหวะการทำงาน(corrupt)เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด

4.3.1 การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด

การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด จัดเป็นความเสี่ยงด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล เนื่องจากเสี่ยงดังกล่าวนั้นเสี่ยงต่อการเข้าถึงข้อมูลที่สำคัญได้ง่าย จึงมีโอกาสที่ข้อมูลจะสูญหายและโอกาสที่ข้อมูลทั้งหมดจะถูกผู้บุกรุกนำออกไปจากระบบมีค่อนข้างสูง เพราะผู้บุกรุกสามารถใช้ความพยายามในการเจาะระบบและขโมยข้อมูลเพียงที่ใดที่หนึ่งของระบบเท่านั้น เมื่อเจาะระบบเข้ามาได้แล้ว ผู้บุกรุกสามารถเข้าถึงข้อมูลสำคัญได้ทั้งหมด จึงสามารถเปลี่ยนแปลงแก้ไขหรือดัดแปลงข้อมูลได้ง่าย นอกจากนี้การเก็บรวบรวมข้อมูลไว้ที่เดียวโดยปราศจากการสำรองข้อมูลไว้ที่อื่นๆ นำไปสู่โอกาสในการสูญเสียข้อมูลสำคัญขององค์กรได้ เพราะในกรณีที่เกิดความผิดพลาดกับระบบ หรือเกิดเหตุขัดข้องที่ทำให้ฐานข้อมูลถูกทำลาย ข้อมูลภายในอาจถูกทำลายและไม่สามารถนำออกมาใช้งานได้ ส่งผลให้องค์กรสูญเสียข้อมูลสำคัญ ต้องเสียเวลาในการรวบรวมข้อมูลใหม่ และกระทบต่อการให้บริการสูงมาก

จากการสำรวจข้อมูลเหตุการณ์ความเสี่ยงเรื่องการเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด กับ กลุ่มตัวอย่างทั้งหมดพบว่าส่วนใหญ่ประเมินว่า โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์กรในเหตุการณ์นี้อยู่ในระดับปานกลาง แต่ประเมินระดับความรุนแรงของความเสี่ยง (Impact) ว่าสูง หากเกิดเหตุการณ์ดังกล่าวในองค์กร

ซึ่งเมื่อเปรียบเทียบระหว่างช่วงอายุการทำงานแล้ว พบว่าแต่ละช่วงมีความคิดเห็นในด้านการประเมินความเสี่ยงแตกต่างกันเช่นเดียวกัน โดยช่วงอายุการทำงานที่มากกว่า 4 ปี ประเมินความเสี่ยง เฉลี่ยว่าอยู่ในระดับสูงซึ่งอาจเป็นเพราะเข้าใจต่อผลกระทบที่จะตามมาหากเกิดเหตุการณ์ดังกล่าวขึ้น

4.3.2 <u>การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้</u>

การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้ จัดเป็นความเสี่ยงการเข้าถึงข้อมูลต่างๆได้เมื่อต้องการใช้งาน ปัญหาของการที่ระบบไม่สามารถให้บริการได้ เช่น การขาดการบำรุงรักษาอุปกรณ์ทางอิเล็กทรอนิกส์ อุปกรณ์ที่ใช้ในการเก็บรักษาและส่งข้อมูลหรืออุปกรณ์ที่ใช้ในการรักษาข้อมูลให้มีสภาพพร้อมใช้งานได้อยู่เสมอ ทำให้เมื่อเกิดเหตุคัดข้องระบบไม่สามารถใช้การได้จึงส่งผลต่อการใช้งานของลูกค้าทั้งจากภายนอกและภายในองค์กร

หรือการเก็บสำรองข้อมูลของระบบอย่างขาดประสิทธิภาพ ทำให้ข้อมูลที่มีอยู่ในระบบจริงกับระบบสำรองไม่ตรงกัน ดังนั้นเมื่อมีการนำเอาข้อมูลจากระบบสำรองมาใช้จึงทำให้เกิดความผิดพลาดได้ การขาดกระบวนการสำรองข้อมูลเพื่อนำมาใช้ในช่วงที่ระบบเกิดปัญหาขัดข้องหรือขาดการบริหารจัดการที่ดีเมื่อเกิดปัญหาระบบไม่สามารถใช้งานได้ ทำให้เกิดความล่าช้าในการกู้ระบบกลับคืนมา

ดังนั้นเมื่อเกิดปัญหาดังกล่าวย่อมส่งผลต่อทั้งลูกค้าและผู้ใช้งานในองค์กรเอง ที่คาดหวังในการใช้บริการระบบ ซึ่งความเสี่ยงดังกล่าวจะส่งผลถึงระดับความพึงพอใจของลูกค้าที่มีต่อระบบหรือบริการขององค์กร และอาจนำไปสู่การสูญเสียลูกค้ารวมทั้งภาพลักษณ์ขององค์กร โดยถ้ามีการพูดปากต่อปาก (Word of mouth) ก็จะทำให้องค์กรสูญเสียลูกค้าได้จำนวนมากในเวลาอันรวดเร็ว

จากการสำรวจข้อมูลเหตุการณ์ความเสี่ยงเรื่องการสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้ กับหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ พบว่าส่วนใหญ่ประเมินว่าโอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์กรในเหตุการณ์นี้อยู่ในระดับปานกลาง แต่ประเมินระดับความรุนแรงของความเสี่ยง (Impact) ว่าสูง หากเกิดเหตุการณ์ดังกล่าวในองค์กร

ซึ่งเมื่อพิจารณาในรายละเอียดพบว่า จากการสำรวจพนักงานหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ ในคำถามดังกล่าว ส่วนใหญ่ที่ประเมินเป็นความเสี่ยงสูงจะอยู่ในช่วงอายุ 20-25 ปี และอายุการทำงานในอายุประมาณช่วง 1-2 ปี

4.3.3 <u>การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล</u>

เหตุการณ์ความเสี่ยง เรื่องการใช้ชื่อ (User ID) จัดอยู่ในกลุ่มความเสี่ยงด้านความเสี่ยงด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล ผลการสำรวจพบว่าโอกาสในการเกิด (Likelihood) เหตุการณ์ดังกล่าวในระดับสูง = 37.27% และระดับปานกลาง= 40% ชี้ให้เห็นว่าการใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูลเป็นเหตุการณ์ที่มีโอกาสเกิดขึ้นได้ในองค์กรค่อนข้างสูง อาจเนื่องจากการเข้าใช้ข้อมูลของพนักงานในองค์กรจะต้องผ่านระบบการตรวจสอบสิทธิการใช้งาน โดยปกติพนักงานแต่ละคนจะมีสิทธิได้รับรหัสประจำตัวเพื่อใช้ในการแสดงตัวตนและขอเข้าใช้ข้อมูลภายในเครือข่ายขององค์กร รหัสประจำตัวสำหรับการเข้าใช้ข้อมูลภายในองค์กรของพนักงานหรือที่เรียกว่า User ID นั้นถูกกำหนดขึ้นโดยเจ้าหน้าที่ดูแลบริหารเครือข่ายและระบบ (Network/System Administrator) ซึ่งทำหน้าที่รวมไปถึงการกำหนดสิทธิการใช้งานข้อมูลต่างๆที่มีอยู่ภายในองค์กร และสิทธิการแก้ไขเปลี่ยนแปลงข้อมูลที่มีในพนักงานแต่ละคนต่างกันไป

ปัญหาคือ เมื่อเกิดเหตุขัดข้องกับระบบหรือข้อมูลภายในระบบ กระบวนการสืบหาผู้มีส่วนเกี่ยวข้องและการเอาผิดกับผู้ที่ก่อปัญหานั้นเป็นเรื่องยาก เนื่องจากรหัสมีผู้ใช้งานมากกว่า 1 คน การตรวจสอบย้อนกลับไปหาผู้ที่เกี่ยวข้องก็ทำได้ยากขึ้น และแม้ว่าระบบสารสนเทศจะถูกออกแบบมาเพื่อให้สามารถสอบกลับหาผู้ใช้งานข้อมูลที่เป็นปัญหาด้วย User ID ที่ทำการล็อกอินเข้ามาได้ แต่ก็อาจจะไม่สามารถหาตัวผู้ใช้ User ID นั้นๆที่แท้จริงได้

นอกจากนี้ปัญหาการใช้ User ID ร่วมกัน ยังรวมไปถึงการที่ผู้บุกรุกหรือผู้ไม่ประสงค์ดีจะสามารถแอบเข้าใช้ User ID ง่ายขึ้นเพราะข้อมูลเกี่ยวกับ User ID และรหัสผ่านถูกเผยแพร่ได้ง่ายเพราะใช้ร่วมกัน เพื่อเข้าใช้เครื่องคอมพิวเตอร์ด้วย User ID ของพนักงานคนใดคนหนึ่งแล้วทำการเปลี่ยนสถานะของเครื่องให้เป็น Super user หรือ Root แล้วใช้ User ID นั้นกลายเป็นฐานในการโจมตีระบบอื่นๆในองค์กรต่อไปได้

ซึ่งปัญหาดังกล่าวโอกาสที่ข้อมูลจะถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่หวังดีมีสูง ไม่ว่าจะโดยตั้งใจหรือไม่ได้ตั้งใจก็ตาม และอาจนำไปสู่ปัญหาการทำงานผิดพลาดของระบบ ซึ่งก่อให้เกิดความล่าช้าในการทำงานหรือร้ายแรงถึงขั้นที่ระบบจะต้องหยุดการทำงานก็ได้

ผลการสำรวจความคิดเห็นเกี่ยวกับความเสี่ยงด้านการใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูลของผู้ใช้ในองค์กรพบว่า

เมื่อเปรียบเทียบระหว่างหน่วยงานที่มีความเกี่ยวข้องกับทางระบบสารสนเทศขององค์กรโดยตรงกับหน่วยงานที่ไม่เกี่ยวข้องนั้นมีความคิดเห็นในด้านการประเมินความเสี่ยงไม่แตกต่างกัน

เปรียบเทียบระหว่างเพศชายและเพศหญิง ก็มีความคิดเห็นในการประเมินความเสี่ยงด้านการใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูลไม่แตกต่างกัน โดยเพศหญิงประเมินเป็นความเสี่ยงสูงมากกว่าเพศชาย

และเมื่อเปรียบเทียบระหว่างช่วงอายุการทำงานแล้ว พบว่าแต่ละช่วงมีความคิดเห็นในด้านการประเมินความเสี่ยงแตกต่างกัน โดยส่วนใหญ่ช่วงอายุการทำงานประมาณ 1-2 ปี ประเมินความเสี่ยง เฉลี่ยว่าอยู่ในระดับสูง

4.3.4 <u>การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม</u>

เหตุการณ์ความเสี่ยง เรื่องการพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุมนั้น ส่วนใหญ่มาจากพฤติกรรมของผู้ใช้งานข้อมูล ในการสั่งพิมพ์ข้อมูลสำคัญหรือข้อมูลความลับ โดยขาดการระแวดระวัง หรือขาดการตระหนักถึงนโยบายในการรักษาความปลอดภัยของข้อมูลในองค์กร และบางส่วนเกิดจากความเข้าใจที่ไม่ตรงกันในการจัดประเภทของข้อมูล ว่าข้อมูลประเภทใดจัดเป็นข้อมูลความลับ ข้อมูลที่จำเป็น หรือข้อมูลทั่วไป จึงทำให้เกิดความเสี่ยงในการสั่งพิมพ์โดยขาดความระมัดระวัง และอาจเกิดข้อมูลที่เป็นความลับถูกเผยแพร่ออกไป ซึ่งจัดเป็นความเสี่ยงด้านความเสี่ยงด้านการรักษาความลับและสิทธิในการเข้าถึงข้อมูล

เพราะเอกสารที่ถูกเผยแพร่ในรูปกระดาษ ถือ เป็นความเสี่ยงด้านข้อมูลอย่างมาก โดยเฉพาะข้อมูลประเภทความลับ หรือข้อมูลเฉพาะขององค์กรที่ห้ามเผยแพร่ โดยปัญหาดังกล่าวส่วนใหญ่มาจากความรู้เท่าไม่ถึงการณ์ของผู้ใช้งานว่าข้อมูลดังกล่าวมีความสำคัญมากน้อยเพียงใด และสามารถจัดพิมพ์ได้หรือไม่เป็นต้น ซึ่งมาจากการขาดความรู้ ความเข้าใจในนโยบายที่เกี่ยวข้องขององค์กรด้วยส่วนหนึ่ง

จากการสำรวจข้อมูลเหตุการณ์ความเสี่ยงเรื่องการพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม กับหน่วยงานที่เกี่ยวข้องกับระบบสารสนเทศ พบว่าส่วนใหญ่ประเมินว่า โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์กรในเหตุการณ์นี้อยู่ในระดับสูง คือประมาณ 47.73%

ของผู้ตอบแบบสอบถามและประเมินระดับความรุนแรงของความเสี่ยง (Impact) ว่าสูงเช่นกัน คือ ประมาณ 40.91% ของผู้ตอบแบบสอบถาม ว่าหากเกิดเหตุการณ์ดังกล่าวในองค์กร

และเมื่อเปรียบเทียบระหว่างช่วงอายุการทำงานแล้ว พบว่าแต่ละช่วงมีความคิดเห็นในด้านการประเมินความเสี่ยงไม่แตกต่างกัน โดยผลสำรวจแยกตามช่วงอายุของพนักงานต่อการประเมินความเสี่ยงเรื่องการพิมพ์ข้อมูลโดยปราศจากการควบคุมไม่แตกต่างกันและผลสำรวจแยกตามเพศก็คิดเห็นไม่แตกต่างเช่นเดียวกัน

4.3.5 <u>ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้</u>

ความเสี่ยงเรื่องผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้ จัดเป็นความเสี่ยงด้านการสามารถเข้าถึงข้อมูลต่างๆได้เมื่อต้องการ ซึ่งเมื่อการสามารถเข้าถึงข้อมูลได้โดยผู้ที่ไม่ได้รับอนุญาตหรือผู้ไม่มีสิทธิ ก็อาจเกิดปัญหาการโจรกรรม แก้ไข ปลอมแปลงหรือเปลี่ยนแปลงข้อมูลเกิดขึ้น ซึ่งส่งผลต่อข้อมูลในระบบที่ใช้งานเกิดการผิดพลาดและอาจส่งผลต่อการใช้งานของลูกค้าในการเรียกดูข้อมูล ย่อมเกิดผลเสียหายอย่างสูงมากเพราะองค์กรเป็นผู้ให้บริการด้านการจัดซื้อ ดังนั้นความถูกต้องของข้อมูลถือว่าสำคัญมากต่อการซื้อขายของลูกค้าผิดพลาดไม่ได้

จากการสำรวจข้อมูลเหตุการณ์ความเสี่ยงเรื่องผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้ พบว่าส่วนใหญ่ประเมินว่า โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์กรในเหตุการณ์นี้อยู่ในระดับต่ำ และประเมินระดับความรุนแรงของความเสี่ยง (Impact) ว่าสูงถึงสูงมาก คือ สูงประมาณ 43.13% สูงมากประมาณ 36.36% จากผู้ตอบแบบสอบถาม หากเกิดเหตุการณ์ดังกล่าวในองค์กร

และพบว่าความคิดเห็นในการประเมินความเสี่ยงของพนักงานในแต่ละช่วงอายุงานๆ ไม่แตกต่างกัน ด้านเพศต่อความคิดเห็นในการประเมินความเสี่ยงก็ไม่แตกต่างเช่นเดียวกัน

ดังนั้น ถึงแม้ปัจจุบันองค์กรจะมีโอกาสเกิดเหตุการณ์การถูกบุกรุกต่ำอยู่ก็ตาม แต่องค์กรก็ไม่อาจละเลยเรื่องการระวังและเตรียมการเตรียมพร้อมอยู่เสมอไม่ได้ เนื่องจากปัจจุบันผู้บุกรุกมีการพัฒนารูปแบบการโจรกรรมและการโจมตีอยู่ตลอดเวลาเช่นกัน ซึ่งหมายความว่าถ้าองค์กรขาดการพัฒนารูปแบบการป้องกันบุกรุกที่ทันสมัยแล้ว องค์กรอาจเกิดผลกระทบอย่างมากเมื่อผู้บุกรุกสามารถเข้าถึงข้อมูลได้ เพราะข้อมูลส่วนใหญ่ขององค์กรเป็นข้อมูลความลับของลูกค้าทั้งสิ้น ซึ่งส่งผลต่อการดำเนินธุรกิจการให้บริการการจัดซื้อออนไลน์ด้วย

4.3.6 Router / Firewall เสียทำให้ไม่สามารถใช้งานได้

ความเสี่ยงเรื่อง Router / Firewall เสียทำให้ไม่สามารถใช้งานได้ จัดเป็นความเสี่ยงด้านการสามารถเข้าถึงข้อมูลต่างๆได้เมื่อต้องการ ซึ่งความเสี่ยงดังกล่าวจะก่อให้เกิดการหยุดชะงักของการใช้งานระบบ เนื่องจากอุปกรณ์เครือข่ายขัดข้องทำให้การเชื่อมต่อไปยังข้อมูลที่ต้องการถูกตัดขาด ระบบป้องกันผู้บุกรุก หยุดทำงานและเสี่ยงต่อการถูกบุกรุกจากผู้ไม่ประสงค์ดีเข้ามาในระบบขณะที่อุปกรณ์เครือข่ายกำลังถูกดำเนินการแก้ไข นอกจากเสี่ยงต่อการถูกบุกรุกจากผู้ไม่ประสงค์ดีในการเข้ามาโจรกรรมและแก้ไขข้อมูลหรือก่อความเสียหายต่อระบบด้านอื่นๆ แล้วนั้น ยังส่งผลการให้บริการลูกค้าหยุดชะงัก การซื้อหรือการให้บริการทางออนไลน์อื่นๆไม่สามารถทำงานได้ ส่งผลเสียต่อการดำเนินธุรกิจทั้งต่อองค์กรเองและลูกค้า

จากการสำรวจข้อมูลเหตุการณ์ความเสี่ยงเรื่อง Router / Firewall เสียทำให้ไม่สามารถใช้งานได้ พบว่าส่วนใหญ่ประเมินว่า โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์กรในเหตุการณ์นี้อยู่ในระดับปานกลาง และประเมินระดับความรุนแรงของความเสี่ยง (Impact) ว่าสูงถึงสูงมาก คือ สูงประมาณ 38.64% สูงมากประมาณ 36.36% จากผู้ตอบแบบสอบถาม หากเกิดเหตุการณ์ดังกล่าวในองค์กร

และพบว่าความคิดเห็นในการประเมินความเสี่ยงของพนักงานในแต่ละช่วงอายุงานๆ ไม่แตกต่างกัน ด้านเพศต่อความคิดเห็นในการประเมินความเสี่ยงก็ไม่แตกต่างเช่นเดียวกัน

4.3.7 <u>ฐานข้อมูล (database) ถูกขัดจังหวะการทำงาน (corrupt) เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด</u>

ความเสี่ยงเรื่องฐานข้อมูล (database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด จัดเป็นความเสี่ยงทางด้านความถูกต้องสมบูรณ์ของข้อมูล เพราะเมื่อฐานข้อมูล (database) ถูกขัดจังหวะการทำงาน (corrupt) เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด ย่อมหมายถึง การที่เครื่อง Server เกิดขัดข้องทำให้ database บนเครื่อง server ดังกล่าวหยุดการทำงานชั่วขณะ จึงส่งผลทำให้ข้อมูลในช่วงเวลาดังกล่าวไม่ถูกเก็บลง database และทำให้การทำงานที่เกี่ยวข้องต้องหยุดตาม ผลที่ตามมาคือข้อมูลที่มีไม่ตรงตามความเป็นจริงเนื่องจากขาดการบันทึกในช่วงเวลาดังกล่าว ดังนั้นเมื่อผู้ใช้งานหรือลูกค้าเรียกข้อมูลดังกล่าวขึ้นมาจึงเป็นข้อมูลที่ผิด กระทบต่อการนำไปใช้งานต่อ รวมทั้งต้องเสียเวลาในการตรวจสอบข้อมูลก่อนการใช้งานทุกครั้ง ขาดความน่าเชื่อถือด้านความถูกต้องของข้อมูล

จากการสำรวจข้อมูลเหตุการณ์ความเสี่ยงเรื่อง เรื่องฐานข้อมูล (database) ถูกขัดจังหวะการทำงาน (Corrupt) เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด พบว่าส่วนใหญ่ประเมิน โอกาสในการเกิดความเสี่ยง (Likelihood) ภายในองค์กรในเหตุการณ์นี้อยู่ในระดับต่ำ และประเมินระดับความรุนแรงของความเสี่ยง (Impact) ว่าอยู่ระดับสูง คือ ประมาณ 54.55% จากผู้ตอบแบบสอบถาม หากเกิดเหตุการณ์ดังกล่าวในองค์กร

และพบว่าความคิดเห็นในการประเมินความเสี่ยงของพนักงานในแต่ละช่วงอายุงานฯ ไม่แตกต่างกัน ด้านช่วงอายุพนักงานต่อการประเมินความเสี่ยงก็ไม่แตกต่างกัน และด้านเพศต่อความคิดเห็นในการประเมินความเสี่ยงก็ไม่แตกต่างเช่นเดียวกัน

ถึงแม้โอกาสในการเกิดความเสี่ยงดังกล่าวในองค์กรจะต่ำแต่องค์กรก็ควรให้ความสนใจเนื่องจากส่งผลต่อภาพลักษณ์ขององค์กรด้วยเช่นกัน ว่าองค์กรขาดการพัฒนาหรือปรับปรุงอุปกรณ์ให้มีความสามารถใช้งานได้ดีตลอดเวลา

สรุปสิ่งที่ควรให้ความสนใจเพิ่มสำหรับผลการสำรวจจากแบบสอบถามพนักงานในองค์กรที่พบสิ่งน่าสนใจและองค์กรควรให้ความสำคัญเช่นเดียวกัน คือ

- พนักงานส่วนใหญ่ 68.18% ทราบว่าองค์กรมีนโยบายด้านการรักษาความปลอดภัยด้านสารสนเทศ แต่จาก 68.18% พบว่า ทราบรายละเอียดของนโยบายดังกล่าว 50% และทราบว่าสามารถเข้าไปอ่านนโยบายดังกล่าวได้จากที่ใด จำนวน 43.64% โดยเมื่อทดสอบสมมติฐานต่อพบว่า ช่วงอายุการทำงานในองค์ที่ต่างกันทำให้มีการทราบนโยบาย รายละเอียดของ

นโยบายและแหล่งที่เก็บ แตกต่างกัน ส่วนสมมติฐานระหว่างพนักงานด้านสารสนเทศและพนักงานทั่วไปไม่พบความแตกต่าง

- พนักงาน 26.36% ทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ขององค์กร สำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศน้อย ถึงน้อยที่สุด และทราบในระดับมากถึงมากที่สุด 24.55% โดยส่วนใหญ่ทราบในระดับปานกลาง โดยเมื่อทดสอบสมมติฐานต่อพบว่า ช่วงอายุการทำงานในองค์ที่ต่างกันทราบเรื่องกฎ ระเบียบ หรือหลักเกณฑ์ ไม่แตกต่างกัน แต่กรณีสมมติฐานระหว่างพนักงานด้านสารสนเทศและพนักงานทั่วไปมีความคิดเห็นแตกต่างกัน

- พนักงาน 46.36% ได้รับการฝึกอบรมหรือรับความรู้ ด้านการรักษาความปลอดภัยด้านระบบสารสนเทศในระดับน้อยถึงน้อยที่สุด และในระดับมากถึงมากที่สุด 13.64% ปานกลาง 40% โดยเมื่อทดสอบสมมติฐานต่อพบว่าช่วงอายุการทำงานในองค์ที่ต่างกันและสมมติฐานระหว่างพนักงานด้านสารสนเทศและพนักงานทั่วไปมีความคิดเห็น ด้านการได้รับการฝึกอบรมไม่แตกต่างกัน

- พนักงาน 50.91% ทราบเรื่องทราบบทลงโทษสำหรับพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความปลอดภัยขององค์กร น้อยถึงน้อยที่สุด และในระดับมากถึงมากที่สุด 10% และปานกลาง 39.09% โดยเมื่อทดสอบสมมติฐานต่อพบว่า ช่วงอายุการทำงานในองค์ที่ต่างกันและสมมติฐานระหว่างพนักงานด้านสารสนเทศและพนักงานทั่วไปมีความคิดเห็นด้านการทราบบทลงโทษสำหรับพนักงานที่ฝ่าฝืนไม่แตกต่างกัน

- พนักงาน 27.27% บอกว่าหน่วยงานของตนเองมีการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงาน (Documented operating procedures)ตามระยะเวลาอันสมควรน้อยถึงน้อยที่สุด โดยเมื่อทดสอบสมมติฐานต่อพบว่า ช่วงอายุการทำงานในองค์กรที่ต่างกันมีความคิดเห็นต่อการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงานของหน่วยงานตนเอง ไม่แตกต่างกัน แต่สมมติฐานระหว่างพนักงานด้านสารสนเทศและพนักงานทั่วไปมีความคิดเห็น ด้านการปรับปรุงคู่มือ ขั้นตอนการปฏิบัติงานของหน่วยงานตนเอง แตกต่างกัน

- พนักงาน 41.82% มีการตรวจสอบอุปกรณ์พ่วงต่อประเภทพกพาต่างๆ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กรมากน้อยเพียงใด ตัวอย่าง การ Scan ไวรัสใน Handy drive ก่อนใช้งานในระดับที่น้อยถึงน้อยที่สุด โดยเมื่อทดสอบสมมติฐานต่อพบว่า ช่วงอายุการทำงานในองค์ที่ต่างกันมีความคิดเห็นต่อการตรวจสอบอุปกรณ์พ่วงต่อ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร ไม่แตกต่างกัน แต่สมมติฐานระหว่างพนักงานด้านสารสนเทศและพนักงานทั่วไปมีความ

คิดเห็น ด้านการการตรวจสอบอุปกรณ์พ่วงต่อ ก่อนทำการใช้งานกับอุปกรณ์ภายในองค์กร แตกต่างกัน

- พนักงาน 41.82% มีการรายงานเหตุการณ์หรือรายงานจุดอ่อน จุดบกพร่องที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่น้อยถึงน้อยที่สุด โดยเมื่อทดสอบสมมติฐานต่อพบว่า ช่วงอายุการทำงานในองค์ที่ต่างกันและสมมติฐานระหว่างพนักงานด้านสารสนเทศและพนักงานทั่วไปมีความคิดเห็น ด้านการรายงานจุดอ่อน จุดบกพร่องที่เกี่ยวกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบไม่แตกต่างกัน

ซึ่งข้อมูลที่พบส่วนใหญ่เป็นเรื่องการขาดการรับรู้ด้านนโยบายและมาตรการต่างๆของที่องค์กรมี การขาดการประชาสัมพันธ์ที่ดีหรือที่กระจายทั่วถึงแก่พนักงานในองค์กร จึงเกิดการรับรู้ที่ไม่ทั่วกันในแต่ละหน่วยงาน รวมทั้งเรื่องการให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของตัวพนักงานเอง

4.4 การวิเคราะห์แนวทางปฏิบัติตาม มาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศ ISO/IEC 17799:2005[9]

จากความเสี่ยงต่างๆที่เกิดขึ้นส่งผลถึงความปลอดภัยข้อมูลขององค์กร ระดับความเสี่ยงที่องค์กรต้องให้ความสำคัญคือความเสี่ยงที่อยู่ในระดับสูง ซึ่งการหาแนวทางควบคุมและปรับปรุงแผนการปฏิบัติงานเพื่อป้องกันการเกิดความเสี่ยงต่อข้อมูล โดยการประยุกต์ใช้มาตรฐานการรักษาความปลอดภัย ISO 17799 สามารถสรุปได้ดังนี้

[9] คณะอนุกรรมการด้านความมั่นคง ใน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์,มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เวอร์ชัน 2,(2549)

4.4.1 แนวทางการควบคุมการเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด

วัตถุประสงค์ : เพื่อให้องค์กรตระหนักถึงความสำคัญในการจัดเก็บข้อมูลและการจัดการข้อมูลสำคัญต่างๆ โดยต้องมีการสำรองข้อมูลที่สำคัญอยู่เสมอ ไม่จัดเก็บรวมกันที่เดียว เพราะหากเกิดความผิดพลาด, เกิดเสียหายต่อฐานในการจัดเก็บข้อมูล (Database) หรือเกิดการบุกรุกจากผู้ไม่มีสิทธิ จะเกิดผลกระทบต่อความมั่นคงปลอดภัยข้อมูลที่เป็นความลับ

สิ่งที่องค์กรตัวอย่างได้ดำเนินการอยู่แล้วในปัจจุบัน : คือ องค์กรมีการสำรองข้อมูลทั้งหมดตามระยะที่กำหนด มีระบบสำรองสำหรับเครื่องเซิร์ฟเวอร์ในทุกๆจุดและมีการระบบสำรองในอีกสถานที่หนึ่ง (Back up Site) เพื่อกรณีที่ระบบที่ให้บริการอยู่หรือระบบสำรองเครื่องเซิร์ฟเวอร์เกิดขัดข้องใช้การไม่ได้หรือมีปัญหาด้านระบบไฟฟ้า ได้มีระบบสำรองให้บริการ

ดังนั้นองค์กรจึงควรมีการจัดการเพิ่มตามแนว ISO 17799 ในการควบคุมความเสี่ยง ดังนี้

1. นโยบายความมั่นคงปลอดภัย (Security policy)

- การเพิ่มการ เผยแพร่ประชาสัมพันธ์ให้พนักงานและผู้เกี่ยวข้องทราบเรื่องนโยบายการจัดเก็บข้อมูลที่สำคัญ และการสำรอง(Back up)ข้อมูลที่สำคัญ เพื่อให้พนักงานตระหนักถึงความสำคัญในการจัดเก็บและรักษาความปลอดภัยแก่ข้อมูลเหล่านั้น

-

2. การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

- โดยการจัดหมวดหมู่สารสนเทศ (Information classification) เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม เช่น การจัดหมวดหมู่ตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

- เพิ่มการจัดฝึกอบรมแก่พนักงานในเรื่องการกำหนดระดับการป้องกันข้อมูล การแบ่งหมวดหมู่ข้อมูล เพื่อเป็นความรู้แก่พนักงานในการดำเนินงานด้านการรักษาความปลอดภัยข้อมูลและช่วยลดความเสี่ยงที่อาจเกิดขึ้นได้จากการเก็บข้อมูลผิดระดับความสำคัญ เป็นต้น

-

3. การระบุตำแหน่งในการจัดเก็บและระบุสิทธิการใช้ข้อมูล

- โดยกำหนดตำแหน่งในการจัดเก็บเพื่อให้ผู้ใช้ข้อมูลที่มีสิทธิเท่านั้นเข้ามาใช้งาน นอกจากนั้นควรมีการระบุระดับสิทธิในการเข้าถึงข้อมูลที่แตกต่างกันให้กับผู้ใช้งานและมีการแจ้ง

อย่างสม่ำเสมอ เช่น สิทธิในการเรียกใช้ข้อมูล สิทธิในการแก้ไขเปลี่ยนแปลง สิทธิในการทำซ้ำการคัดลอก สิทธิในการอ่านและสิทธิในการลบข้อมูลเป็นต้น โดยสำรวจสิทธิจากการใช้งานจริงและความต้องการของผู้ใช้งานแต่ละคนก่อน เพื่อระบุระดับได้เหมาะสม

- ซึ่งปัจจุบันองค์กรที่ศึกษาก็ได้มีการควบคุมโดยวิธีการแบ่งสิทธิการเข้าถึงข้อมูลที่แตกต่างกันอยู่ จึงควรให้ความสนใจเพิ่มในการปรับปรุงและแก้ไขสิทธิให้ทันสมัยอยู่เสมอ เช่น การเปลี่ยนสิทธิเมื่อมีพนักงานย้ายหน่วยงานหรือลาออก เป็นต้น และแจ้งสิทธิการใช้งานที่แตกต่างกันแก่ผู้ใช้งานสม่ำเสมอ

-

4. <u>การสำรองข้อมูล(Information back-up)</u>

- มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ โดยองค์กรควรจัดทดสอบข้อมูลที่สำรองเก็บไว้หรือในระบบสำรอง (Back up Site) อย่างสม่ำเสมอและให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กรเองสำหรับเป็นแนวทางการป้องกันความเสี่ยงและการสูญหายของข้อมูล หากเกิดการบุกรุกและโจรกรรม หรือจากภัยธรรมชาติ เพราะข้อมูลที่ถูกสำรองจะถูกนำมาใช้งานแทนข้อมูลที่ถูกทำลายหรือโจรกรรมไป เป็นการลดผลกระทบต่อการไม่สามารถเข้าถึงข้อมูลได้ทางหนึ่ง

-

5. <u>การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)</u>

- จุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กรโดย

- การจัดทำบริเวณล้อมรอบ (Physical security perimeter) คือ มีการจัดสรรพื้นที่กั้นบริเวณที่เหมาะสม เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรและควบคุมการเข้า-ออก (Physical entry controls)ในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้นเพื่อลดความเสี่ยงต่อจากการบุกรุกเข้าถึงข้อมูลซึ่งองค์กรตัวอย่างได้มีการดำเนินอยู่ในปัจจุบัน

4.4.2 แนวทางการควบคุมการสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้

วัตถุประสงค์ : เพื่อให้องค์กรตระหนักถึงความสำคัญของการที่ระบบจะไม่ทำงานหรือไม่สามารถให้บริการต่อลูกค้าทั้งทางตรงและทางอ้อม เพื่อรักษามาตรฐานการให้บริการ รักษาฐานลูกค้าเดิม และรักษาภาพลักษณ์ขององค์กร

สิ่งที่องค์กรตัวอย่างได้ดำเนินการอยู่แล้วในปัจจุบัน คือ องค์กรมีระบบสำรอง(Back up Site) ที่เก็บรักษาข้อมูลที่ใช้ในการให้บริการเก็บอีกสถานที่หนึ่ง เพื่อให้บริการกรณีเกิดปัญหา มีการกำหนดสิทธิในการเข้าใช้ห้องเซิร์ฟเวอร์หรือห้องที่เก็บข้อมูลสำคัญ ให้เฉพาะผู้ที่เกี่ยวข้องหรือผู้ที่มีสิทธิเท่านั้น เช่น มีการใช้บัตรผ่าน การป้อนรหัสผ่าน รวมทั้งการใช้เครื่องตรวจลายนิ้วมือ เป็นต้น

แนวทางการควบคุมสำหรับความเสี่ยงดังกล่าวเพิ่มเติมตาม ISO 17799 สามารถแบ่งได้ดังนี้

1. การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)

- โดยการจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ เพื่อเตรียมความพร้อมป้องกันก่อนเกิดภัยต่างๆ ซึ่งส่งผลต่อระบบที่จะไม่สามารถให้บริการแก่ลูกค้าได้

-

2. การบริหารจัดการโครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External Parties)

- จัดทำข้อกำหนดในการให้บริการ(Service Level Agreement) หรือ SLA ของการให้บริการ เพื่อตอบสนองความพึงพอใจของลูกค้าในการที่จะได้รับบริการและความช่วยเหลือตามข้อตกลง โดยข้อตกลงนี้เป็นปัจจัยหนึ่งในการสร้างความมั่นใจให้กับลูกค้าว่าจะสามารถรับบริการหรือเข้าใช้ข้อมูลได้ตามเวลาที่องค์กรกำหนด หรือการสามารถแก้ปัญหาที่เกิดขึ้นได้อย่างรวดเร็วภายในระยะเวลาที่ลูกค้ายอมรับได้ ซึ่งการที่องค์กรจะเสนอข้อตกลงการให้บริการ สิ่งสำคัญที่ต้องคำนึงถึงคือ ความสามารถของระบบขององค์กรที่จะสามารถกลับมาใช้งานได้ตามปกติเมื่อเกิดปัญหาใดๆขึ้นมา

- องค์กรควรมีการปรับปรุงข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร สำหรับลูกค้า ผู้ใช้บริการ หรือผู้ให้บริการระบบ จากภายนอก ในการเข้าถึง

สารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ให้สอดคล้องกับนโยบายและเป้าหมายขององค์กร สม่ำเสมอ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

- องค์กรควรจัดให้มีระบบสำรองเครือข่ายข้อมูล(ระบบอินเตอร์เน็ต – ISP) เผื่อในกรณีที่เครือข่ายหลักใช้งานไม่ได้ ได้สามารถใช้ระบบเครือข่ายจากอีกผู้ให้บริการ

-

3. <u>การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)</u>

- มีจุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

- ควรจัดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process) คือ การกำหนดให้มีการบริหารจัดการและการปรับปรุงกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจไว้ด้วย

- ควรจัดให้มีการประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment) คือการระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อเตรียมแผนรองรับหรือเตรียมการป้องกันล่วงหน้า

- ควรให้มีการจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)และการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว เช่น การกำหนดแผนกู้ข้อมูล (Recovery Plan) เมื่อระบบเกิดปัญหา โดยการจัดทำแผนจะต้องแน่ใจว่าข้อมูลและโปรแกรมประยุกต์ (Application) ต่างๆ จะถูกกู้กลับมาใช้งานได้ตามเดิมอย่างถูกต้อง โดยการใช้ข้อมูลที่ได้ทำการเก็บสำรองไว้โดยผู้ดูแลระบบ เป็นต้น

- ซึ่งตัวอย่างดังกล่าวเป็นเพียงวิธีการเชิงแก้ไขกรณีเมื่อเกิดเหตุการณ์ขึ้นแล้ว เพื่อเป็นการพยายามให้เกิดช่วงเวลาที่ระบบไม่สามารถใช้งานได้หรือไม่สามารถให้บริการลูกค้าได้ ให้

น้อยที่สุด ระบบจึงต้องสามารถกลับมาใช้งานได้ตามปกติให้เร็วที่สุดเท่าที่จะเป็นได้ เพื่อสร้างความพึงพอใจแก่ลูกค้าหรือผู้ใช้งาน

- ควรมีการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework) เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน สามารถครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และเป็นการจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการ รวมทั้งควรให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี เช่น การตรวจสอบและเฝ้าระวัง(Audit and Monitoring) เป็นต้น สำหรับการแก้ไขปัญหาได้อย่างทันท่วงที ซึ่งการตรวจสอบทำได้หลายลักษณะ อย่างการตรวจสอบข้อมูลที่ถูกใช้งาน รหัสผู้ใช้งาน ลักษณะการใช้งานข้อมูล เพื่อเก็บเป็นข้อมูลในการป้องการใช้ข้อมูลที่ผิดปกติ มีแนวโน้มก่อเกิดปัญหา

โดยการตรวจสอบและเฝ้าระวังความเสี่ยงรวมทั้งภัยคุกคามต่างๆ เพื่อเป็นการลด "Down time" ให้ต่ำที่สุด ดังนั้นองค์กรจึงต้องคอยเฝ้าระวังดูแลความปลอดภัยของระบบอยู่ตลอดเวลา ซึ่งในปัจจุบันองค์กรทั่วโลกเริ่มนิยมใช้บริการ "IT Security Outsourcing" จาก MSSP หรือ "Managed Security Services Provider" กันมากขึ้นเนื่องจากช่วยประหยัดค่าใช้จ่ายให้แก่องค์กรโดยรวมได้ ซึ่งองค์กรสามารถควบคุมคุณภาพของ MSSP โดยกำหนด SLA (Service Level Agreement) ที่รัดกุม และ ชัดเจน ก็จะช่วยให้การทำงานร่วมกันระหว่างองค์กรและ MSSP เป็นไปอย่างราบรื่น และมีประสิทธิภาพมากที่สุด

4.4.3 <u>แนวทางการควบคุมการใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล</u>

<u>วัตถุประสงค์</u> : เพื่อให้องค์กรตระหนักถึงความสำคัญของปัญหาที่จะตามมาในการใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้งานต่างๆ

<u>สิ่งที่องค์กรตัวอย่างได้ดำเนินการอยู่แล้วในปัจจุบัน</u> คือ องค์กรมีการกำหนดสิทธิการใช้งานระบบที่แตกต่างไปในแต่ละบุคคล สำหรับในการเข้าใช้งานโปรแกรม Application และการเรียกดูข้อมูลเพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว

รวมทั้งองค์กรตัวอย่างมีการกำหนดระยะเวลาในการเปลี่ยนรหัสผ่าน(Password) และการกำหนดห้ามใช้รหัสผ่านที่ซ้ำกับที่เคยใช้แล้ว

ดังนั้นสิ่งที่องค์กรควรดำเนินการเพิ่มเติมเพื่อควบคุมความเสี่ยงดังกล่าว คือ

1. <u>การกำหนดนโยบายให้ชัดเจนและการประชาสัมพันธ์ที่เหมาะสม</u>

เพื่อสร้างความเข้าใจระหว่างองค์กรและพนักงานให้ตรงกัน ซึ่งสาเหตุส่วนใหญ่เกิดการขาดการตระหนักถึงผลเสียหรือผลกระทบที่จะตาม ขาดการให้ความสำคัญและการจัดการที่เข้มงวด ดังนั้นเพื่อเป็นการลดโอกาสของความเสี่ยงที่จะเกิดจากการใช้ User ID รวมกันคือ

- องค์กรควรมีการควบคุมพร้อมทั้งจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งานอยู่เสมอ
- องค์กรควรมีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) โดยจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เช่น ในการขอเพิ่มสิทธิ หรือเปลี่ยนแปลงสิทธิ เป็นต้นเพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งาน
- องค์กรควรมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ตามระยะเวลาที่กำหนดไว้สม่ำเสมอ

2. <u>การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)</u>

- องค์กรควรมีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานเป็นลายลักษณ์อักษร เพื่อเป็นการแจ้งให้รับทราบโดยทั่วกัน ในป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ เช่น การกำหนดว่าพนักงานจะต้องรับผิดชอบต่อการกระทำทั้งหมดที่เกิดขึ้น จากการเข้าใช้ข้อมูลด้วย User ID ของตนเอง หรือพนักงานมีหน้าที่ในการรักษาความปลอดภัยด้านสารสนเทศขององค์กร ดังนั้นพนักงานต้องไม่เปิดเผย User ID และ Password ของตนให้ผู้อื่นทราบยกเว้น ได้รับอนุญาตจากผู้บังคับบัญชาหรือกรณีฉุกเฉินเท่านั้น เป็นต้น
- องค์กรควรมีการจัดทำข้อกำหนดการใช้งานรหัสผ่าน (Password use)โดยการกำหนดวิธีปฏิบัติที่ดี สำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน

3. <u>การจัดฝึกอบรมและให้ความรู้แก่พนักงาน</u>

- องค์กรควรมีการจัดฝึกอบรมและให้ความรู้แก่พนักงานในองค์กร เพื่อสร้างความเข้าใจที่ตรงกันระหว่างพนักงานและองค์กรในการปฏิบัติงาน มีการอบรมข้อแนะนำในการปฏิบัติ

งาน การใช้งาน Application ต่างๆในองค์กร รวมทั้งอธิบายความสำคัญของการดูแลรักษาความลับของ User ID และ Password ของตน

- องค์กรควรมีการอธิบายถึงผลกระทบและความเสี่ยงต่างที่จะตามมา หากขาดการระมัดระวังในเรื่องดังกล่าวเกิดขึ้น เพื่อให้ทุกคนตระหนักถึงผลเสียหรือปัญหาที่จะตามภายหลัง

4.4.4 <u>แนวทางการควบคุมการพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม</u>

<u>วัตถุประสงค์</u> : เพื่อให้ทุกคนที่ทำงานให้แก่องค์กรรับรู้ถึงความสำคัญของข้อมูลต่างๆที่จัดเก็บว่าสามารถเผยแพร่หรือนำออกได้มากน้อยเพียงใด และรู้จักสิทธิของตนในการใช้ข้อมูลประเภทต่างๆ รวมทั้งสร้างมาตรฐานในการวิเคราะห์ความสำคัญของข้อมูลต่างๆ การแยกประเภทของมูล แก่ทุกแผนกในองค์กรให้เท่าเทียมกัน

ซึ่งการควบคุมความเสี่ยงตามมาตรฐาน ISO17799 สามารถทำได้ ดังนี้

1. <u>การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment)</u>

- เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

- องค์กรควรมีการสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training) คือ ต้องกำหนดให้พนักงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอก ได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย เช่น การอบรม ในการจัดประเภทของข้อมูลต่างๆขององค์กรเพื่อสร้างความเข้าใจที่ตรงกันทั้งในการจัดเก็บ การรักษา การนำไปใช้ การจัดพิมพ์ เป็นต้น

2. <u>การควบคุมการเข้าถึง สำหรับสารสนเทศ (Business requirements for access control)</u>

- องค์กรควรมีการจัดทำนโยบายการควบคุมการเข้าถึงระบบ (Access control policy)อย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ รวมทั้งการกำหนดบทลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

- องค์กรควรมีการบริหารจัดการการเข้าถึงของผู้ใช้ (User access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ในการเข้าใช้หรือจัดพิมพ์เอกสารที่สำคัญๆขององค์กร

- องค์กรควรมีการควบคุมการพิมพ์เอกสาร (Printing Control) โดยการกำหนดควบคุมและจำกัดสิทธิต่างๆ ในเข้าใช้และจัดการข้อมูลตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติ ซึ่งองค์กรอาจนำเอาซอฟแวร์ เข้ามาช่วยในการบริหารจัดการ การใช้และการจัดการข้อมูลหรือเอกสาร เพื่อให้สามารถทำการตรวจสอบย้อนถึงผู้จัดพิมพ์ เวลาที่สั่งพิมพ์หรือจำนวนครั้งที่สั่งพิมพ์เอกสารที่มีค่านั้น และเพื่อสามารถกำหนดการทำงานกับไฟล์ข้อมูลหรือเอกสารดังกล่าว เช่น สิทธิเฉพาะการอ่านเอกสาร สิทธิในการแก้ไข สิทธิในการสั่งพิมพ์ เป็นต้น ซึ่งถ้าผู้ไม่มีสิทธิก้อไม่สามารถทำการใดๆกับไฟล์ดังกล่าวได้

- องค์กรควรมีการประกาศแจ้งถึงสิทธิต่างๆในการพิมพ์เอกสาร บทลงโทษ เพื่อให้พนักงานรับทราบถึงความสำคัญในการรักษาข้อมูลต่างๆในองค์กร และเพื่อให้พนักงานรู้สึกถึงการรับผิดชอบร่วมกันหากเกิดปัญหา

- องค์กรควรมีการให้ความรู้หรือฝึกอบรมแก่พนักงานอย่างสม่ำเสมอ ในการจัดการข้อมูลต่างๆภายในองค์กร ในการแบ่งประเภทและความสำคัญของข้อมูลประเภทต่างๆว่าสามารถนำออกมาแพร่หรือจัดพิมพ์ได้มากน้อยเพียงใด

3. <u>การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) เพื่อลดความเสี่ยง</u>

ในการเข้าถึงข้อมูลหรือเอกสารลับเฉพาะขององค์กร(Confidential Document) ซึ่งวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน คือ

1). รหัสผ่านจะต้องไม่บอกให้ผู้อื่นทราบไม่ว่าในกรณีใดๆ

2). รหัสผ่านต้องมีมากกว่า 8 อักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

3). ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้พจนานุกรม

4). ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

5). ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่

6). ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกต เห็นของบุคคลอื่น

7). พนักงานต้องลงนามเพื่อเก็บรักษา รหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

8). ต้องกำหนดรหัสผ่านเริ่มต้นให้ยากต่อการเดาและการส่งมอบรหัสผ่านให้กับพนักงานต้องเป็นไปอย่างปลอดภัย

- และควรมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบ (Review of user access rights)อย่างเป็นทางการตามระยะเวลาที่กำหนดไว้ เพื่อควบคุมสิทธิการเข้าถึงข้อมูลที่สำคัญให้เหมาะสมกับการใช้งานเสมอ

4. <u>การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling)</u>

- เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต

- องค์กรควรมีการกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศ(Information handling procedures)เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์ รวมทั้งกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต(Security of system documentation)

- องค์กรควรมีการแยกเก็บข้อมูลที่สำคัญหรือลับเฉพาะออกจากข้อมูลทั่วไป และกำหนดสิทธิเฉพาะผู้ที่จำเป็นหรือเกี่ยวข้องเท่านั้น

4.4.5 <u>แนวทางการควบคุมผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้</u>

วัตถุประสงค์ : เพื่อให้องค์กรตระหนักถึงผลกระทบที่จะตามมา เมื่อระบบที่ให้บริการถูกบุกรุกจากผู้ไม่ประสงค์ดี และเพื่อเป็นแนวทางในการป้องกันผู้บุกรุกหรือ ผู้ไม่ประสงค์ดีทั้งจากภายในและภายนอก ในการโจรกรรม แก้ไข ปลอมแปลงหรือเปลี่ยนแปลงข้อมูล

สิ่งที่องค์กรตัวอย่างได้ดำเนินการอยู่แล้วในปัจจุบัน คือ องค์กรมีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนัง จัดทำประตูทางเข้า-ออกที่มีการควบคุมด้วยระบบอิเล็กทรอนิกส์ เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร สำหรับการป้องกันโปรแกรมที่ไม่ประสงค์ดี ปัจจุบันองค์กรตัวอย่าง มีการติดตั้งโปรแกรมป้องกันไวรัสทั้งในเครื่องคอมพิวเตอร์และโน้ตบุ๊ก ที่มีการอัพเดทโปรแกรมเป็นประจำทุกวัน

องค์กรจึงควรให้ความสนใจ 2 ด้านใหญ่ๆ คือ การควบคุมการเข้าถึง (Access control) และการสร้างความปลอดภัยทางกายภาพ โดยมีรายละเอียดดังนี้

1. การควบคุมการเข้าถึง (Access control)

- องค์กรควรมีนโยบายการควบคุมการเข้าถึงระบบ (Access control policy)อย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความแผนและกลยุทธ์ขององค์กรทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

- องค์กรควรมีการบริหารจัดการการเข้าถึงของผู้ใช้ (User access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและมีสิทธิแล้วเท่านั้น มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน และมีการจัดทำเอกสารแจ้งสิทธิอย่างเป็นลายลักษณ์อักษร รวมทั้งมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานเสมอ

- องค์กรควรมีการแจ้งหน้าที่ความรับผิดชอบแก่ผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ โดยการนำการใช้งานรหัสผ่าน (Password use)

- องค์กรควรมีการประชาสัมพันธ์แก่พนักงานในการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)เพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น คอมพิวเตอร์ เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น

- องค์กรควรมีการจัดให้มีการควบคุมการเข้าถึงเครือข่าย (Network access control)เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต เช่น การจัดทำนโยบายการ

ใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้

- องค์กรควรมีการแบ่งแยกเครือข่าย (Segregation in networks) ตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เพื่อป้องการ การเข้าถึงจากบุคคลที่ไม่มีส่วนเกี่ยวข้องหรือไม่มีสิทธิและแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

- องค์กรควรมีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยจัดให้มีขั้นตอนปฏิบัติในการเข้าถึงระบบหรือการเข้าใช้งานระบบปฏิบัติการ ที่เหมาะสมในการรักษาคามั่นคงปลอดภัย เช่น การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

- องค์กรควรมีการกำหนดการหมดเวลาใช้งานระบบสารสนเทศ (Session time-out)หรือให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้ และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง เพื่อป้องกันผู้บุกรุกจากการเปิดทิ้งไว้โดยไม่ใช้งานเป็นเวลา

- องค์กรควรมีการการควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต สามารถทำโดย การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)และฟังก์ชันต่างๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งานและความจำเป็นที่เหมาะสม

- องค์กรควรมีการควบคุมอุปกรณ์สื่อสารประเภทพกพา(เช่น notebook, palm, และ laptop เป็นต้น) เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร เช่น การกำหนดมาตรการตรวจสอบไวรัส ในอุปกรณ์ต่อพ่วงทุกก่อนนำเข้ามาใช้งานกับอุปกรณ์ภายในองค์กร

2. <u>การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)</u>

ปัจจุบันองค์กรตัวอย่างมีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกที่มีการควบคุม เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผล

สารสนเทศขององค์กรจากผู้ไม่เกี่ยวข้อง โดยอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น และมีการลงชื่อของผู้เข้าใช้งานพร้อมเวลาเข้า-ออก

- ดังนั้นองค์กรควรมีการแจ้งพนักงานในการขอความร่วมมือ ในการลงทะเบียนเข้า-ออกในสถานที่ที่กำหนดให้มีการลงชื่อ ขอให้พนักงานใช้บัตรของตนเองในการเข้า-ออก ประตูตามห้องควบคุมต่างๆ เพื่อเวลาเกิดปัญหาได้ตามผู้มีส่วนเกี่ยวข้องได้

- องค์กรควรมีการแจ้งพนักงานในการขอความร่วมมือสำหรับการจัดวางและป้องกันอุปกรณ์ต่างๆของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

3. <u>การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)</u>

ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย โดยผู้ดูแลระบบ ซึ่งมีรายละเอียดดังนี้

- องค์กรควรมีการติดตั้งและใช้งานซอฟต์แวร์ป้องกันไวรัส หนอน และม้าโทรจันเพื่อป้องกันความเสียหายของข้อมูล โดยมีการปรับปรุงในทันต่อการพัฒนาของไวรัสและมีการสแกนทั้งเครื่องแม่ข่าย คอมพิวเตอร์และโน้ตบุ๊ก โดยปัจจุบันองค์กรตัวอย่างได้ดำเนินการอยู่แล้ว

- องค์กรควรมีการฝึกอบรมให้ตระหนักถึงความสำคัญของการป้องกันไวรัส หนอน และม้าโทรจัน รวมทั้งการตรวจสอบเบื้องต้น วิธีสังเกตข้อมูลหรืออีเมล์ที่คาดว่าไม่ประสงค์ดี การดึงข้อมูลและแฟ้มจากอินเตอร์เน็ตต้องได้รับการดูแลที่ดีเพื่อป้องกันโปรแกรมที่ไม่พึงประสงค์และสิ่งที่ไม่เหมาะสมเข้ามา

- ระบบฮาร์ดแวร์ ซอฟต์แวร์ ระบบปฏิบัติการ โปรแกรมต่างๆ ระบบเน็ตเวิร์คและระบบสื่อสารต้องได้รับการจัดการที่เหมาะสมและได้รับการดูแลป้องกันต่อสู้ทั้งการโจมตีและการละเมิดการใช้เน็ตเวิร์คโดยไม่ได้รับอนุญาต

- องค์กรควรให้พนักงานตระหนักถึงการรับอีเมล์ ที่ต้องได้รับการดูแลตามลักษณะความเสี่ยงประเภทข้อมูล ว่าการเปิดอีเมล์ที่มีแฟ้มแนบต้องมีการสแกนไวรัสหรือโปรแกรมที่ไม่พึงประสงค์อื่นๆ ก่อนทุกครั้ง

- องค์กรควรแจ้งแก่พนักงาน ว่าแฟ้มคอมพิวเตอร์จากผู้ที่ไม่ประสงค์ออกนามต้องลบโดยไม่มีการเปิดอ่านใดๆทั้งสิ้น

ซึ่งทั้งหมดต้องอาศัยการประชาสัมพันธ์แก่พนักงานในองค์กร เพื่อตระหนักถึงผลกระทบและร่วมมือในการดำเนินงานเพื่อการป้องกันความปลอดภัยของข้อมูล

โดยปัจจุบันองค์กรตัวอย่างได้มีจัดทำมาตรการรองรับสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดีเช่น ไวรัส รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย โดยการแจ้งข่าวสาร ข้อมูลความรู้ต่างๆรวมทั้งวิธีการป้องกันผ่านช่องทางที่กำหนดในองค์กร

4.4.6 <u>แนวทางการควบคุม Router / Firewall เสียทำให้ไม่สามารถใช้งานได้</u>

<u>วัตถุประสงค์</u> : เพื่อให้องค์กรเตรียมพร้อมในการรองรับหากเกิดกรณีฉุกเฉิน เมื่อระบบป้องกันที่ใช้งานอยู่ไม่สามารถใช้การได้ พร้อมตระหนักถึงความสำคัญและผลที่อาจตามมา

<u>สิ่งที่องค์กรตัวอย่างได้ดำเนินการอยู่แล้วในปัจจุบัน</u> คือ องค์กรมีการบำรุงรักษาอุปกรณ์ (Equipment maintenance) อย่างสม่ำเสมอตามระยะเวลาที่กำหนด จากหน่วยงานภายนอกที่มีความชำนาญ

องค์กรจึงควรมีการเตรียมพร้อมเพื่อลดปัญหาจากความเสียหาย หรือการใช้งานไม่ได้ของอุปกรณ์เชื่อมต่อเครือข่าย ทั้งRouter, Firewall และอุปกรณ์ที่สำคัญอื่นๆคือ

1. <u>การบริหารจัดการทรัพย์สินขององค์กร (Asset management)</u>

- องค์กรควรมีการกำหนดหน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets) เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหาย ที่อาจเกิดขึ้นได้ ควรมีการกำหนดการใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)เช่น การจัดทำกฎระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหาย อันเกิดจากการขาดความระมัดระวัง การขาดการดูแลและเอาใจใส่ เป็นต้น
- ซึ่งปัจจุบัน องค์กรตัวอย่างได้มีการจัดทำกฎระเบียบและหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและแจ้งแก่บุคคลภายในองค์กรผ่านทางอีเมล์ ส่วนอุปกรณ์ที่เกี่ยวข้องกับการประมวลผลสารสนเทศยังไม่มีเป็นเอกสารที่ระบุเพื่อป้องกันความเสียหายที่ชัดเจน เป็นเพียงการบอกกล่าวในการทำงาน

2. <u>การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)</u>

- องค์กรควรมีการบำรุงรักษาอุปกรณ์ (Equipment maintenance) ที่ต้องมีการดูแลและบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน เช่น มีการตรวจสอบสภาพอุปกรณ์อย่างน้อย 1 ครั้งในระยะเวลา 6 เดือน

- ความเสียหายที่เกิดกับทรัพย์สินขององค์กรควรมีการรายงานเพื่อตรวจหาสาเหตุและความผิดพลาดที่เกิดจากอุปกรณ์เน็ตเวิร์คต้องมีการรายงานและบันทึกเก็บไว้

- อุปกรณ์เน็ตเวิร์คขององค์กรควรมีได้รับการตรวจสอบก่อนใช้จริงและการเคลื่อนย้ายอุปกรณ์เน็ตเวิร์คควรมีการทำประกันที่เหมาะสมเพื่อป้องกันการสูญหาย ถูกทำลาย หรือถูกขโมยได้

- องค์กรควรมีการเตรียมอุปกรณ์หรือแผนสำรองฉุกเฉิน หากเกิดเหตุการณ์ที่อุปกรณ์เชื่อมต่อด้านเครือข่ายไม่ทำงาน

- องค์กรควรมีการบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management) เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิค โดยการกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

3. <u>การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)</u>

- มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

- องค์กรควรมีมาตรการทางเครือข่าย (Network controls)ในการบริหารและจัดการเครือข่าย ด้วยการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอพพลิเคชั่นที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย

- ซึ่งปัจจุบันองค์กรตัวอย่างมีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ที่จะเข้ามาทำความเสียหายแก่ เครือข่ายและแอพพลิเคชั่นต่างๆไว้แล้ว

- องค์กรควรมีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมด (Security of

network services) ที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่าย โดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในองค์กร

4.4.7 <u>แนวทางการควบคุมฐานข้อมูล (database) ถูกขัดจังหวะการทำงาน (corrupt) เนื่องจากฮาร์ดแวร์และซอฟแวร์ทำงานผิดพลาด</u>

<u>วัตถุประสงค์</u> : เพื่อให้องค์กรตระหนักถึงความสำคัญของการที่ระบบจะไม่ทำงานหรือไม่สามารถให้บริการต่อลูกค้าทั้งทางตรงและทางอ้อม เพื่อรักษามาตรฐานการให้บริการ รักษาฐานลูกค้าเดิม และรักษาภาพลักษณ์ขององค์กร

<u>สิ่งที่องค์กรตัวอย่างได้ดำเนินการอยู่แล้วในปัจจุบัน</u> คือ องค์กรมีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอในเรื่องของระบบ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร อีกทั้งปัจจุบันผู้บังคับบัญชาจะคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กรแต่ยังไม่เข้มงวดมากสำหรับหน่วยงานที่ไม่มีส่วนเกี่ยวข้องกับสื่อสารสนเทศและอุปกรณ์ในการประมวลผลขององค์กร

1. <u>การสำรองข้อมูล (Information back-up)</u>

องค์กรควรมีการจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศ โดยมีรายละเอียดดังนี้

- หัวหน้างานสารสนเทศกำหนดระยะเวลาในการสำรองข้อมูลที่เหมาะสม เช่น สำรองข้อมูลเป็นประจำทุกชั่วโมง หรือทุกสัปดาห์ แล้วแต่ประเภทข้อมูล เป็นต้น
- หัวหน้างานสารสนเทศต้องมั่นใจว่ามีการสำรองข้อมูลและกระบวนการกู้ระบบที่เหมาะสมก่อนการรีสตาร์ททุกครั้ง
- ผู้บริหารต้องให้ความสำคัญในการสำรองข้อมูลและความสามารถในการกู้ข้อมูลเพื่อความมั่นใจว่าสามารถตอบสนองความต้องการทางธุรกิจได้
- โดยปัจจุบันองค์กรตัวอย่างมีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ โดยเก็บและดูแลข้อมูลในเครื่องเซิร์ฟเวอร์เป็นประจำทุกวัน

2. <u>การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)</u>

- องค์กรควรมีการจัดให้มีการการรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses) เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กร ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม โดยการให้พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร รายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรหรือจุดอ่อนที่พบเห็น ผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้

- เพื่อการแก้ไขและพัฒนาปรับปรุงอุปกรณ์รวมทั้งจุดอ่อนที่พบ ก่อนเกิดปัญหาที่จะส่งผลกระทบต่อองค์กร

- ซึ่งปัจจุบันองค์กรตัวอย่างก็ได้มีการจัดเก็บและรวบรวมหลักฐานรวมถึงข้อมูล log ต่างๆในการดำเนินงานไว้ตลอด