ผนวก ข

มาตรฐานการบริหารจัดการการให้บริการ ISO / IEC 20000

เนื่องด้วยมีการนำเอาระบบเทคโนโลยีสารสนเทศเข้ามาใช้จำนวนมาก จึงทำให้งานทางด้านบริการทางด้านเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญ เพราะจะต้องคอยให้บริการแก่ผู้ที่ขอรับบริการในด้านต่างๆ ไม่ว่าจะเป็นการแก้ไขปัญหา การแนะนำวิธีการใช้งานอุปกรณ์และอื่นๆ และเพื่อให้ผู้รับบริการได้รับความมั่นใจว่าผู้ให้บริการเหล่านั้นจะสามารถดำเนินงานได้อย่างมั่นคง ต่อเนื่อง และมีเสถียรภาพที่ดี จึงได้มีการจัดทำมาตรฐานการบริหารจัดการการให้บริการ ISO / IEC 20000 ขึ้น โดยแต่เดิมคือ BS 15000 ซึ่งเกิดขึ้นที่ประเทศอังกฤษ และได้รับการพัฒนาจนในปัจจุบันได้กลายเป็นมาตรฐานระดับนานาชาติ คือ ISO / IEC 20000 โดยมีองค์ประกอบดังนี้

ภาพที่ 2 แสดงองค์ประกอบของกระบวนการที่เกี่ยวข้องกับการบริหารจัดการการให้บริการ

<table>
<tr><td colspan="3">กระบวนการให้บริการ</td></tr>
<tr><td>การบริหารจัดการขีดความสามารถของระบบ</td><td>การบริหารจัดการระดับการให้บริการ</td><td>การบริหารจัดการด้านความมั่นคงปลอดภัย</td></tr>
<tr><td>การบริหารจัดการการให้บริการเพื่อให้บริการได้อย่างต่อเนื่อง</td><td>การจัดทำรายงานการให้บริการ</td><td>การจัดทำงบประมาณและบัญชีสำหรับค่าใช้จ่ายในการให้บริการ</td></tr>
<tr><td colspan="3">กระบวนการควบคุม
การบริหารจัดการการปรับแต่งระบบการบริหารจัดการการเปลี่ยนแปลง</td></tr>
<tr><td>กระบวนการส่งมอง</td><td></td><td>ระบวนการสร้างความสัมพันธ์</td></tr>
<tr><td>การบริหารจัดการการส่งมอบ</td><td>ขาดความต่อเนื่องในการดำเนินงาน
การบริหารจัดการปัญหาการใช้งาน</td><td>การบริหารจัดการเพื่อสร้างความสัมพันธ์กับองค์กร
การบริหารจัดการผู้นำปัจจัยเข้าสำหรับการผลิต</td></tr>
</table>

1. กระบวนการให้บริการ

1.1 การบริหารจัดการระดับการให้บริการ

กระบวนการนี้มีวัตถุประสงค์เพื่อกำหนด ตกลงซึ่งกันและกัน บันทึก และบริหารจัดการระดับการให้บริการ ขอบเขตทั้งหมดของการให้บริการจะต้องได้รับการตกลงกันระหว่างผู้ที่เกี่ยวข้องทั้งหมดในการให้บริการแต่ละชนิด (หรือแต่ละประเภท) จะต้องถูกกำหนดหรือควบคุมโดยข้อตกลงการให้บริการหรือที่เรียกกันว่า Service Level Agreement (SLA) เช่น ในการให้บริการแก้ไขปัญหาเกี่ยวกับกรใช้งานเครื่องคอมพิวเตอร์ ผู้ให้บริการและผู้ใช้บริการอาจร่วมกันกำหนดข้อตกลงการให้บริการ เช่น การให้บริการแก้ไขปัญหาไวรัสจะต้องดำเนินการให้แล้วเสร็จภายใน 4 ชั่วโมงนับตั้งแต่ได้รับแจ้งเข้ามา

ระดับการให้บริการจะต้องได้รับการเฝ้าระวังและรายงานตามเป้าหมายที่ได้กำหนดไว้ เช่น ทุกครั้งที่ได้รับแจ้งปัญหาไวรัส ผู้ให้บริการจะต้องบันทึกข้อมูลการแก้ไขปัญหาและระยะเวลาที่ใช้ในการแก้ไขปัญหาเก็บไว้ ซึ่งสามารถนำไปสู่การทำรายงานสรุประยะเวลาโดยเฉลี่ยในการแก้ไขปัญหาไวรัสแต่ละครั้ง

1.2 การจัดทำรายงานการให้บริการ

เพื่อจัดทำรายงานที่เกี่ยวข้องกับการให้บริการ รายงานอาจประกอบด้วย

- ประสิทธิภาพเมื่อเทียบกับเป้าหมายการให้บริการที่กำหนดไว้ (เช่น การแก้ไขปัญหาไวรัสภายใน 4 ชั่วโมง เป็นต้น)
- ความไม่สอดคล้อง (เช่น กับข้อตกลงการให้บริการ) และประเด็นที่เกี่ยวข้อง เช่น ด้วยข้อตกลงการให้บริการแก้ไขปัญหาไวรัสภายใน 4 ชั่วโมง บางกรณีของการแก้ไขปัญหาไวรัสอาจใช้ระยะเวลาในการแก้ไขเกินกว่า 4 ชั่วโมง ซึ่งมีสาเหตุมาจากฮาร์ตดิสก์ได้รับความเสียหาย และต้องสั่งซื้อฮาร์ตดิสก์ลูกใหม่ เป็นต้น
- ข้อมูลที่เกี่ยวข้องกับเวิร์คโหลดของระบบ เช่น ข้อมูลปริมาณการใช้ดิสก์และซีพียูของเซิร์ฟเวอร์ป้องกันไวรัส เป็นต้น
- ประสิทธิภาพของระบบหลังจากที่มีเหตุการณ์สำคัญฯ เกิดขึ้น เช่น ประสิทธิภาพของระบบภายหลังจากที่มีการแพร่ระบาดของไวรัสเกิดขึ้น เป็นต้น
- ข้อมูลการวิเคราะห์ความพึงพอใจ

1.3 การบริหารจัดการการให้บริการเพื่อให้บริการได้อย่างต่อเนื่อง

เพื่อให้ผู้บริการมีหน้าที่ผูกพันกับการให้บริการอย่างต่อเนื่องภายใต้สถานการณ์ต่างๆ ที่เกิดขึ้น องค์กรต้องจัดทำแผนการสร้างความต่อเนื่องสำหรับการให้บริการ โดยอาจพิจารณาข้อมูลจากแผนทางธุรกิจ ข้อตกลงการให้บริการ และผลการประเมินความเสี่ยง ซึ่งแผนสร้างความต่อเนื่องดังกล่าว ควรได้รับการทดสอบและปรับปรุงให้ดีขึ้นอย่างสม่ำเสมอ

1.4 การจัดทำงบประมาณและบัญชีสำหรับค่าใช้จ่ายในการให้บริการ

เพื่อกำหนดงบประมาณและทำบัญชีค่าใช้จ่ายในการให้บริการ โดยองค์กรจะต้องมีกระบวนการที่ชัดเจนในการทำบัญชีค่าใช้จ่าย เพื่อคิดค่าใช้จ่ายในการให้บริการ เช่น ผู้ให้บริการอาจคิดค่าใช้จ่ายในการให้บริการแก้ไขปัญหาไวรัสต่อครั้ง การคิดค่าใช้จ่ายดังกล่าว อาจพิจารณาจากงบประมาณที่จำเป็นต้องใช้ในการดำเนินการ เช่น ค่า License สำหรับซอฟต์แวร์ป้องกันไวรัส ค่าฮาร์ดแวร์และอุปกรณ์ต่างๆ ค่าจ้างบุคล ค่าโสหุ้ย และอื่นๆ การคิดค่าใช้จ่ายต้องมีรายละเอียดที่เพียงพอเพื่อให้การอนุมัติและการตัดสินใจดำเนินการต่างๆ เป็นไปอย่างสัมฤทธิผล

อย่างไรก็ตาม สำหรับผู้ให้บริการภายในองค์กร โดยทั่วไปจะไม่มีการคิดค่าใช้จ่ายในการให้บริการต่างๆ ดังนั้นกระบวนการในหัวข้อนี้อาจไม่มีการใช้งาน

1.5 การบริหารจัดการขีดความสามารถของระบบ

เพื่อให้ผู้ให้บริการมีขีดความสามารถหรือทรัพยากรที่พอเพียงต่อการให้บริการ เพื่อให้สามารถตอบสนองต่อความต้องการขององค์กรทั้งในปัจจุบันและอนาคต โดยองค์กรจะต้องจัดทำแผนการเพิ่มขีดความสามารถ เช่น เป็นแผนรายปี ซึ่งประกอบด้วยความต้องการทรัพยากรสารสนเทศเพิ่มเติมสำหรับปีนั้น

การบริหารจัดการขีดความสามารถของระบบ มีองค์ประกอบที่เกี่ยวข้องได้แก่

- การกำหนดความต้องการประสิทธิภาพและขีดความสามารถทั้งในปัจจุบันและอนาคตที่คาดการณ์ไว้
- การกำหนดช่วงระยะเวลาและค่าใช้จ่ายในการปรับปรุงการให้บริการ เช่น การปรับปรุงเซิร์ฟเวอร์ป้องกันไวรัสจะดำเนินการในช่วงระยะเวลาใด
- การประเมินผลกระทบจากการปรับปรุงการให้บริการ ซึ่งรวมถึงการเปลี่ยนแปลงเทคโนโลยีหรือเทคนิกใหม่ๆ เพื่อเพิ่มขีดความสามารถของระบบ
- การมีกระบวนการและข้อมูลเพื่อใช้ในการวิเคราะห์ความต้องการขีดความสามารถเพิ่มเติม

องค์กรต้องมีวิธีการ ขั้นตอนการปฏิบัติ และเทคนิกที่จำเป็น เพื่อคอยเฝ้าระวังและตรวจสอบขีดความสามารถของระบบหรือการให้บริการ ปรับปรุงประสิทธิภาพในการให้บริการ และมีการเพิ่มขีดความสามารถของระบบอย่างเพียงพอ

1.6 การบริหารจัดการด้านความมั่นคงปลอดภัย

เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยสำหรับกิจกรรมการให้บริการทั้งหมด การบริหารจัดการด้านความมั่นคงปลอดภัยสามารถอ้างอิงจากแนวทางการปฏิบัติของมาตรฐานระดับนานาชาติ ISO / IEC 17799 โดยองค์กรจะต้องจัดทำและอนุมัตินโยบายด้านความมั่นคงปลอดภัย รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดซึ่งรวมถึงลูกค้าและผู้ให้บริการ ได้รับทราบ

ในการแก้ไขปัญหาไวรัสขององค์กร ส่วนหนึ่งของนโยบายด้านความมั่นคงปลอดภัยอาจกล่าวถึงนโยบายการป้องกันไวรัส เช่น

- พนักงานต้องติดตั้งโปรแกรมป้องกันไวรัสตามที่องค์กรกำหนดไว้ และตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ
- พนักงานต้องทำการตรวจสอบไวรัสในเครื่องที่ตนใช้งาน สัปดาห์ละครั้ง
- พนักงานต้องรายงานปัญหาไวรัสที่พบให้เจ้าหน้าที่ Help desk ทราบโดยเร่งด้วน เป็นต้น

นโยบายนี้ควรเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบและปฏิบัติตามนอกจากนั้นแล้วองค์กรจะต้อง

- กำหนดมาตรการความมั่นคงปลอดภัยที่จำเป็นและสอดคล้องกับนโยบายความมั่นคงปลอดภัย
- กำหนดให้มีการประเมินบริหาร และจัดการความเสี่ยงอย่างสม่ำเสมอ เนปีละครั้ง

ในการแก้ไขปัญหาไวรัสขององค์กร มาตรการความมั่นคงปลอดภัยที่เกี่ยวข้องเพื่อเตรียมความพร้อมขององค์กร ได้แก่

- การติดตั้งเซิร์ฟเวอร์ป้องกันไวรัส
- การติดตั้งโปรแกรมป้องกันไวรัสเครื่องลูกข่ายขององค์กร
- การกำหนดให้ผู้ใช้ทำการรายงานปัญหาไวรัสที่พบ โดยเร่งด่วนต่อเจ้าหน้าที่ Help desk
- การกำหนดขั้นตอนปฏิบัติเพื่อรับมือกับปัญหาไวรัส

มาตรการทั้งหมดนี้เป็นมาตรการด้านความมั่นคงปลอดภัยที่สอดคล้องกับนโยบายการป้องกันไวรัส

2. กระบวนการสร้างความสัมพันธ์

2.1 การบริหารจัดการเพื่อสร้างความสัมพันธ์กับองค์กร

เพื่อสร้างความสัมพันธ์ที่ดีระหว่างผู้ให้บริการและองค์กร โดยจะต้องทบทวนการให้บริการของผู้ให้บริการในรอบระยะเวลาที่ผ่านมา และอาจนำไปสู่การเปลี่ยนแปลงต่อขอบเขต ข้อตกลงการให้บริการ และ/หรือสัญญาการให้บริการ ผู้ให้บริการและองค์กรอาจมีการจัดประชุมย่อยเป็นครั้งคราวตามรอบระยะเวลาที่ตกลงกันไว้ เพื่อหารือกันในประเด็นต่างๆ โดยการประชุมทุกครั้งที่จัดขึ้นจะต้องมีการบันทึกไว้เป็นลายลักษณ์อักษร

ผู้ให้บริการและองค์กรจะต้องจัดให้มีกระบวนการในการรับปัญหาที่ร้องเรียนมาจากผู้ใช้บริการ ปัญหาที่ร้องเรียนมาจะต้องได้รับการบันทึกไว้โดยผู้ให้บริการ สืบสวนสอบสวน แก้ไขปัญหา รายงานให้ผู้ที่เกี่ยวข้องได้รับทราบ และปิดปัญหาที่ร้องเรียนมา ผู้ให้บริการต้องแต่งตั้งผู้ที่มีหน้าที่รับผิดชอบในการบริหารจัดการความพึงพอใจของผู้ใช้บริการ รวมทั้งกระบวนการสร้างความสัมพันธ์กับผู้ใช้บริการ

2.2 การบริหารจัดการผู้นำปัจจัยเข้าสำหรับการผลิต

เพื่อบริหารจัดการผู้นำปัจจัยสำหรับการผลิตขององค์กร เพื่อให้การให้บริการของผู้นำปัจจัยเข้าไปอย่างมีคุณภาพ โดยผู้ให้บริการจะต้องกำหนดกระบวนการบริหารจัดการผู้นำปัจจัยเข้าอย่างชัดเจน และเป็นลายลักษณ์อักษร รวมทั้งกำหนดผู้ทำหน้าที่รับผิดชอบในสัญญาระห่างผู้ให้บริการและผู้นำปัจจัยเข้า ข้อกำหนดในการให้บริการ ขอบเขต ระดับของการให้บริการโดยผู้นำปัจจัยเข้า และกระบวนการในการติดต่อสื่อสารกันจะต้องได้รับการบันทึกไว้อย่างเป็นลายลักษณ์อักษรในข้อตกลงการให้บริการระหว่างผู้ให้บริการและผู้นำปัจจัยเข้า โดยข้อตกลงการให้บริการผู้นำปัจจัยเข้าจะต้องเป็นไปในทิศทางเดียวกัน หรือไม่ขัดยังกับข้อตกลงการให้บริการโดยผู้ให้บริการต่อองค์กร

บทบาทและความสัมพันธ์ระหว่างผู้นำปัจจัยเข้าหลัก และผู้นำปัจจัยเข้ารายย่อย ต้องได้รับการบันทึกไว้อย่างเป็นลายลักษณ์อักษร รวมทั้งผู้นำปัจจัยเข้าหลักจะต้องมีกระบวนการเพื่อแสดงให้เห็นว่า ผู้นำปัจจัยเข้ารายย่อยจะปฏิบัติตามข้อกำหนดที่ระบุไว้ในสัญญาการให้บริการ ผู้ให้บริการต้องมีกระบวนการเพื่อจัดการกับการโต้แย้งระหว่างผู้ให้บริการและผู้นำปัจจัยเข้า และจะต้องมีกลไกการเฝ้าระวังและทบทวนประสิทธิภาพการให้บริการของผู้นำปัจจัยเข้า รวมทั้งกำหนดการดำเนินการเพิ่มเติมเพื่อปรับปรุงประสิทธิภาพให้ดีขึ้นต่อไป

3. กระบวนการแก้ไขปัญหา

3.1 การบริหารจัดการเหตุการณ์ที่ทำให้ขาดความต่อเนื่องในการดำเนินการ

เพื่อบริหารจัดการกับเหตุการณ์ที่ทำให้ขาดความต่อเนื่องในการดำเนินงาน กระบวนการนี้จะมุ่งเน้นไปที่การกู้ระบบหรือธุรกิจให้กลับคืนสู่สภาวะปกติให้เร็วที่สุดเท่าที่จะทำให้ได้ ในหลายๆ องค์กร ผู้ปฏิบัติกระบวนการนี้คือ Help desk หรือ Service desk โดยเหตุการณ์ดังกล่าวต้องได้รับการบันทึกไว้ องค์กรต้องมีขั้นตอนปฏิบัติเพื่อบริหารจัดการผลกระทบขอบเหตุการณ์ดังกล่าว ขั้นตอนปฏิบัติจะต้องมีองค์ประกอบได้แก่ การบันทึกเหตุการณ์ การจัดลำดับความสำคัญ การประเมินผลกระทบ การจัดหมวดหมู่เหตุการณ์ การดำเนินการขั้นต่อไปหากเหตุการณ์ที่แจ้งมายังไม่ได้รับการแก้ไข การแก้ไขเหตุการณ์ และปิดเหตุการณ์ โดยผู้รับบริการจะต้องได้รับแจ้งถึงความก้าวหน้าของการแก้ไขเหตุการณ์ รวมทั้งระดับการให้บริการที่อาจลดต่ำลงในช่วงระยะเวลาที่กำลังดำเนินการแก้ไขเหตุการณ์ดังกล่าว

3.2 การบริหารจัดการปัญหาการใช้งาน

เพื่อลดการหยุดชะงักต่อธุรกิจ และให้สามารถใช้งานได้อย่างต่อเนื่อง โดยมุ่งเน้นไปที่การระบุและวิเคราะห์หาสาเหตุของเหตุการณ์ที่ทำให้ขาดความต่อเนื่อง เพื่อป้องกันการเกิดขึ้นซ้ำของเหตุการณ์หรือข้อผิดพลาดเดียวกันขึ้นอีก โดยองค์กรจะต้องดำเนินการเชิงป้องกัน เพื่อลดปัญหาที่มีโอกาสเกิดขึ้น เช่น ศึกษาจากแนวโน้มของปัญหาที่เกิดขึ้นในช่วงระยะเวลาที่ผ่านมา การแก้ไขปัญหาต้องได้รับการเฝ้าระวัง ทบทวน และรายงานสถานภาพการดำเนินการ เพื่อให้เกิดความมัมฤทธิผลในการแก้ไขปัญหา

4. กระบวนการควบคุม

4.1 การบริหารจัดการการปรับแต่ระบบ

เพื่อกำหนดและควบคุมองค์ประกอบที่เกี่ยวข้องกับการปรับแต่งระบบ รวมทั้งบำรุงรักษาข้อมูลการปรับแต่ระบบให้มีความถูกต้อง องค์กรจะต้องกำหนดรายการทั้งหมดของข้อมูลสำหรับการปรับแต่ง ความสัมพันธ์ของข้อมูลการปรับแต่ง และเอกสารที่เกี่ยวข้องกับการปรับแต่ง การบริหารจัดการการปรับแต่งระบบจะต้องมีกลไกการระบุ ควบคุม และสามารถตรวจสอบเวอร์ชั่นของการปรับแต่งนั้นได้ กลไกการควบคุมการปรับแต่งต้องพอเพียงและเหมาะสม โดยพิจารณาถึงความจำเป็นของธุรกิจ และความเสี่ยงอันเกิดจากความล้มเหลวในการปรับแต่ง และระดับความสำคัญของบริการที่เกี่ยวข้อง โดยการบริหารจัดการการปรับแต่งระบบจะต้องให้ข้อมูลกับกระบวนการการบริหารจัดการการเปลี่ยนแปลงในเชิงผลกระทบที่อาจเกิดขึ้นกับการเปลี่ยนแปลง

ต่อข้อมูลการปรับแต่งระบบ การเปลี่ยนแปลงต่อข้อมูลดังกล่าวต้องสามารถตรวจสอบได้ว่าใครเป็นผู้ดำเนินการ ทำการเปลี่ยนแปลงอะไร เมื่อไร เป็นต้น

ขั้นตอนการปฏิบัติเพื่อควบคุมการปรับแต่งจะต้องรักษาหรือคงไว้ซึ่งความสมบูรณ์ของระบบต่างๆ ที่เกี่ยวข้อง องค์กรจะต้องเก็บข้อมูลการปรับแต่ง และต้องเก็บไว้ในสถานที่มีความปลอดภัย โดยข้อมูลที่มีการปรับแต่งในแต่ละครั้งที่ดำเนินการจะต้องสามารถระบุแยกออกจากกันได้ และได้รับการบันทึกไว้ในฐานข้อมูลการปรับแต่งระบบ รวมทั้งมีการควบคุมการเข้าถึงฐานข้อมูลดังกล่าว และสามารถตรวจสอบความถูกต้องของฐานข้อมูลนี้ได้ด้วย

4.2 การบริหารจัดการการเปลี่ยนแปลง

เพื่อให้มีการประเมิน อนุมัติ ลงมือปฏิบัติ และทบทวนการเปลี่ยนแปลงต่อเทคโนโลยีสารสนเทศ โดยจะต้องมีการกำหนดขอบเขตอย่างชัดเจน และเป็นลายลักษณ์อักษร โดยการขอเปลี่ยนแปลงแต่ละครั้งจะต้องได้รับการบันทึกและจัดหมวดหมู่ไว้ และจะต้องได้รับการประเมินในแง่ของความเสี่ยง ผลกระทบ และข้อดีที่มีต่อธุรกิจ โดยกระบวนการบริหารจัดการการเปลี่ยนแปลงจะต้องสามารถยกเลิกและย้อนกลับไปสู่ระบบเดิมก่อนการแก้ไขนั้นในกรณีที่การเปลี่ยนแปลงนั้นไม่สำเร็จด้วยสาเหตุใดสาเหตุหนึ่งก็ตาม และการเปลี่ยนแปลงจะต้องได้รับการอนุมัติ ตรวจสอบ และหลังจากนั้นจึงจะสามารถลงมือปฏิบัติตามที่ร้องขอมาได้ โดยองค์กรจะต้องมีนโยบายและขั้นตอนการปฏิบัติเพื่อควบคุมการอนุมัติ และการลงมือปฏิบัติสำหรับกรณีการขอเปลี่ยนแปลงฉุกเฉิน

5. กระบวนการส่งมอบ

5.1 การบริหารจัดการส่งมอบ

เพื่อส่งมอบบริการ ระบบ ซอฟแวร์ ฮาร์ตแวร์ หรืออื่นๆ ไปสู่กรใช้งานจริง โดยผู้ให้บริการจะต้องวางแผนร่วมกับองค์กรในการส่งมอบบริการ ระบบ ซอฟแวร์ ฮาร์ตแวร์ หรืออื่นๆ เพื่อไปสู่การใช้งานจริง แผนการส่งมอบต้องได้รับความเห็นชอบ และอนุมัติโดยทุกหน่วยงานที่มีส่วนเกี่ยวข้อง กระบวนการส่งมอบจะต้องสามารถยกเลิกและย้อนกลับไปสู่ระบบเดิมได้ ในกรณีที่ไม่สามารถทำได้สำเร็จตามแผนการส่งมอบ และนอกจากนี้ผู้ให้บริการจะต้องจัดเตรียมระบบสำหรับการทดสอบ เพื่อใช้ในการทดสอบก่อนที่จะส่งมอบบริการ ระบบ ซอฟแวร์ ฮาร์ตดิส หรืออื่นๆ ไปสู่การใช้งานจริง การส่งมอบเพื่อไปสู่การติดตั้ง และใช้งานจะต้องระมัดระวังในทุกขั้นตอน เพื่อไม่ให้ซอฟแวร์และฮาร์ตแวร์ที่เกี่ยวข้องถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต นับตั้งแต่การหีบห่อ การจัดการ การส่งมอบ และการติดตั้ง