**แบบสอบถามการควบคุมภายใน**

**ด้านระบบเทคโนโลยีสารสนเทศในการบริหารจัดการ**

| **คำถาม** | **มี/ใช่** | **ไม่มี/ไม่ใช่** | **คำอธิบาย/คำตอบ** |
| --- | --- | --- | --- |
| **๑. นโยบายด้านความมั่นคงปลอดภัยของระบบสารสนเทศภายในหน่วยงาน**  **วัตถุประสงค์ของการควบคุม**  *เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร ให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฎิบัติที่เกี่ยวข้อง โดยผู้บริหารองค์กรจะต้องมีการจัดทำนโยบายที่เป็นลายลักษณ์อักษร รวมถึงการทบทวนนโยบายตามระยะเวลาที่กำหนดหรือมีการเปลี่ยนแปลงที่สำคัญขององค์กร*  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุงการควบคุมภายใน ให้ดีขึ้น*ดังนี้  ........................................................................................................  ........................................................................................................  **๒. โครงสรางทางดานความมั่นคงปลอดภัยของระบบสารสนเทศ**  **วัตถุประสงค์ของการควบคุม**  *เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก*  ๒.๑ โครงสรางทางดานความมั่นคงปลอดภัยภายในหน่วยงาน  ๒.๑.๑ มีการมอบหมายแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบกำหนดเป็นลายลักษณ์อักษรด้านความมั่นคงปลอดภัย  ๒.๑.๒ มีการบริหารจัดการความมั่นคงปลอดภัยภายในหน่วยงาน  ๒.๑.๓ มีกระบวนการในการอนุมัติการใชงานอุปกรณด้านเทคโนโลยีสารสนเทศ  ๒.๑.๔ มีกระบวนการจัดการกับข้อมูลที่กำหนดชั้นความลับให้เป็นไปตามระเบียบข้อบังคับที่เกี่ยวข้อง  ๒.๒ โครงสรางทางดานความมั่นคงปลอดภัยที่เกี่ยวของกับการให้บริการต่างๆ  ๒.๒.๑ มีการประเมินความเสี่ยงการเข้าถึงระบบสารสนเทศจากหน่วยงานภายนอก สำหรับหน่วยงานที่ให้บริการสารสนเทศแก่บุคคลหรือหน่วยงานภายนอก  ๒.๒.๒ มีการระบุขอกําหนดสําหรับผูใชบริการที่เกี่ยวของกับความมั่นคงปลอดภัยสําหรับสารสนเทศของหน่วยงาน  **สรุป โครงสรางทางดานความมั่นคงปลอดภัยของระบบสารสนเทศ**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุง การควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๓. การบริหารจัดการสินทรัพย์ด้านสารสนเทศของหน่วยงาน**  **วัตถุประสงค์ของการควบคุม**  *เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจขึ้นได้และ*  *มีการกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม*  ๓.๑ หนาที่ความรับผิดชอบต่อสินทรัพย์ฯ ของหน่วยงาน  ๓.๑.๑ มีการจัดทําบัญชีสินทรัพย์  ๓.๑.๒ มีการระบุผูดูแล ผู้รับผิดชอบ ผู้ใช้สินทรัพย์  ๓.๑.๓ มีการกำหนดการใช้สินทรัพย์อย่างเหมาะสม  ๓.๒ การจัดหมวดหมู่ระบบงานสารสนเทศ (Software ; Information classification)  ๓.๒.๑ มีการจัดหมวดหมูระบบงานสารสนเทศ  ๓.๒.๒ สามารถระบุหมวดหมู่ระบบงานสารสนเทศได้โดยง่าย  **สรุป การบริหารจัดการสินทรัพย์ด้านสารสนเทศของหน่วยงาน**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุง การควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๔. ความมั่นคงปลอดภัยที่เกี่ยวของกับบุคลากร**  **วัตถุประสงค์ของการควบคุม**  *เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิด*  ๔.๑ ความมั่นคงปลอดภัยที่เกี่ยวของกับบุคลากรภายนอก  ๔.๑.๑ มีการสรางความมั่นคงปลอดภัยกอนการจางงานบุคคลภายนอก (Prior to employment)  ๔.๑.๑.๑ มีการกําหนดกรอบปฎิบัติด้านความมั่นคงปลอดภัย  ๔.๑.๑.๒ มีการตรวจสอบคุณสมบัติของผูรับจ้าง  ๔.๑.๒ การสรางความมั่นคงปลอดภัยในระหวางการจางงานบุคคลภายนอก (During employment)  ๔.๑.๒.๑ มีการกำหนดหนาที่ในการบริหารจัดการทางดานความมั่นคงปลอดภัย  ๔.๑.๒.๒ มีการสรางความตระหนัก การใหความรู และการอบรมดานความมั่นคงปลอดภัยใหแกพนักงาน  ๔.๑.๒.๓ มีการระบุความรับผิดทางกฎหมาย  ๔.๑.๓ การสิ้นสุดหรือการเปลี่ยนการจางงานบุคคลภายนอก (Termination or change of employment)  ๔.๑.๓.๑ มีการกำหนดการสิ้นสุดหรือการเปลี่ยนการจางงาน  ๔.๑.๓.๒ มีการคืนทรัพยสินของหน่วยงาน  ๔.๑.๓.๓ มีการถอดถอนสิทธิในการเขาถึงสถานที่ อุปกรณ์ และระบบสารสนเทศ  ๔.๒ ความมั่นคงปลอดภัยที่เกี่ยวของกับบุคลากรภายใน  ๔.๒.๑ มีการกําหนดหนาที่ความรับผิดชอบดานความมั่นคงปลอดภัย  ๔.๒.๒ มีการให้และถอดถอนสิทธิ์ในการเข้าถึงสถานที่ อุปกรณ์ ระบบสารสนเทศ และคืนสินทรัพย์เมื่อมีการโยกย้าย  ๔.๒.๓ มีการสรางความตระหนัก การใหความรู และการอบรมดานความมั่นคงปลอดภัยใหแกบุคลากรภายในหน่วยงาน  ๔.๒.๔ มีกระบวนการลงโทษทางวินัย  **สรุป ความมั่นคงปลอดภัยที่เกี่ยวของกับบุคลากร**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุงการควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๕. การสรางความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดลอม**  **วัตถุประสงค์ของการควบคุม**  *เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร*  ๕.๑ บริเวณที่ตองมีการรักษาความมั่นคงปลอดภัย (Secure areas)  ๕.๑.๑ มีการกำหนดขอบเขตพื้นที่โดยเฉพาะ  ๕.๑.๒ มีการกำหนดมาตรการควบคุมการเขา-ออก  ๕.๑.๓ มีมาตรการรักษาความมั่นคงปลอดภัยสําหรับสํานักงานหองทํางานและสินทรัพย์อื่นๆ  ๕.๑.๔ มีมาตรการปองกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม  ๕.๑.๖ มีการกำหนดพื้นที่เฉพาะสําหรับการติดต่อของบุคคลภายนอก  ๕.๒ ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)  ๕.๒.๑ มีการจัดวางและการปองกันอุปกรณ  ๕.๒.๒ มีระบบและอุปกรณสนับสนุนการทํางานประเภท UPS อุปกรณ์สำรองข้อมูล อุปกรณ์สำรองไฟฟ้า และอื่น ๆ  ๕.๒.๓ มีการเดินสายไฟฟ้า สายสัญญาณสื่อสาร และสายเคเบิ้ลอื่นๆ อย่างเรียบร้อยปลอดภัย  ๕.๒.๔ มีการดูแลบํารุงรักษาอุปกรณ  ๕.๒.๕ มีการปองกันอุปกรณที่ใชงานอยูนอกสํานักงาน  ๕.๒.๖ มีการกำจัดอุปกรณ์ที่ชำรุดหรือการนำอุปกรณ์ที่ผ่านการซ่อมบำรุงกลับมาใช้งาน  ๕.๒.๗ มีมาตรการควบคุมการนําทรัพยสินของหน่วยงานออกนอกหน่วย  **สรุป การสรางความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดลอม**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุงการควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๖. การบริหารจัดการเครื่องแม่ข่ายและการดำเนินงานของเครือข่ายสารสนเทศ**  **วัตถุประสงค์ของการควบคุม**  *เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย*  ๖.๑ การกําหนดหนาที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน  ๖.๑.๑ มีขั้นตอนการปฏิบัติงานที่เปนลายลักษณอักษร  ๖.๑.๒ มีการควบคุมการเปลี่ยนแปลงปรับปรุงหรือแกไขระบบหรือ อุปกรณประมวลผลสารสนเทศ  ๖.๑.๓ มีการแบงหนาที่ความรับผิดชอบ  ๖.๑.๔ มีการแยกระบบและอุปกรณ์สําหรับการพัฒนา การทดสอบ และการใหบริการออกจากกัน  ๖.๒ มีการวางแผนและการกำหนดความต้องการทรัพยากรสารสนเทศ  ๖.๓ มีการปองกันโปรแกรมที่ไมประสงคดี  ๖.๔ มีการสํารองขอมูล (Back-up)  ๖.๕ มีการบริหารจัดการโดยมีมาตรการความมั่นคงปลอดภัยทางระบบ  ๖.๖ มีมาตรการจัดการสื่อที่ใชในการบันทึกขอมูล (Media handling) (การกำจัด การทำลาย การเก็บรักษา การอนุญาต และการใช้งาน)  ๖.๗ การแลกเปลี่ยนข้อมูลสารสนเทศ (Exchange of information)  ๖.๗.๑ มีนโยบายและขั้นตอนปฏิบัติสําหรับการแลกเปลี่ยนข้อมูลสารสนเทศ  ๖.๗.๒ มีขอตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศ  ๖.๗.๓ มีการสงสื่อบันทึกขอมูลออกไปนอกหน่วยงาน  ๖.๗.๔ มีการสงขอความ/แฟ้มข้อมูลทางอิเล็กทรอนิกส์  ๖.๘ การเฝาระวังทางดานความมั่นคงปลอดภัย (Monitoring)  ๖.๘.๑ มีการบันทึกเหตุการณที่เกี่ยวของกับการใชงานระบบสารสนเทศ  ๖.๘.๒ มีการตรวจสอบการใชงานระบบสารสนเทศ  ๖.๘.๓ มีการปองกันขอมูลบันทึกเหตุการณ์  ๖.๘.๔ มีบันทึกกิจกรรมการดําเนินงานของเจาหนาที่ ที่เกี่ยวของกับระบบสารสนเทศ  ๖.๘.๕ มีการบันทึกเหตุการณขอผิดพลาด  ๖.๘.๖ มีการตั้งเวลาของเครื่องคอมพิวเตอรใหตรงกัน  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุง การควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๗. การควบคุมการเขาถึงระบบสารสนเทศและฐานข้อมูล**  **วัตถุประสงค์ของการควบคุม**  *เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต*  ๗.๑ การบริหารจัดการ การควบคุม และเข้าถึงระบบสารสนเทศของผู้ใช้  ๗.๑.๑ มีนโยบายและมาตรการการควบคุมการเข้าถึงระบบสารสนเทศ  ๗.๑.๒ มีการลงทะเบียนผู้ใช้งาน  ๗.๑.๓ มีการบริหารจัดการสิทธิการใชงาน  ๗.๑.๔ มีการบริหารจัดการรหัสผานสําหรับผูใชงาน  ๗.๑.๕ มีการทบทวนสิทธิการเขาถึงของผูใชงาน  ๗.๒ การกำหนดหนาที่ความรับผิดชอบของผูใชงาน อุปกรณ์ที่ไม่มีเจ้าหน้าที่ดูแล (User responsibilities)  ๗.๒.๑ มีการใชงานรหัสผาน  ๗.๒.๒ มีการกำกับดูแลควบคุมและป้องกันไมทิ้งทรัพยสินสารสนเทศสําคัญไวในที่ที่ไมปลอดภัย  ๗.๓ การควบคุมการเขาถึงเครือขาย (Network access control)  ๗.๓.๑ มีมาตรการใชงานบริการเครือขาย  ๗.๓.๒ มีการพิสูจนตัวตนสําหรับผูใชที่อยูภายนอกหน่วยงาน  ๗.๓.๓ มีการพิสูจนตัวตนอุปกรณบนเครือขาย  ๗.๓.๔ มีการปองกันพอรตที่ใชสําหรับตรวจสอบและปรับแตงระบบ  ๗.๓.๕ มีการแบงแยกเครือขาย  ๗.๓.๖ มีการควบคุมการเชื่อมตอทางเครือขาย  ๗.๓.๗ มีการควบคุมการกําหนดเสนทางบนเครือขาย  ๗.๔ การควบคุมการเขาถึงระบบปฏิบัติการ (Operating system access control)  ๗.๔.๑ มีขั้นตอนปฏิบัติในการเขาถึงระบบอยางมั่นคงปลอดภัย  ๗.๔.๒ มีการระบุและพิสูจนตัวตนของผูใชงาน  ๗.๔.๓ มีระบบบริหารจัดการรหัสผาน  ๗.๔.๔ มีการใชงานโปรแกรมประเภทยูทิลิตี้  ๗.๔.๕ มีการหมดเวลาการใชงานระบบสารสนเทศ  ๗.๔.๖ มีการจํากัดระยะเวลาการเชื่อมตอระบบสารสนเทศ  ๗.๕ การควบคุมการเขาถึงแอพพลิเคชั่นและสารสนเทศ (Application and information access control)  ๗.๕.๑ มีการจํากัดการเขาถึงสารสนเทศ  ๗.๕.๒ มีการแยกระบบสารสนเทศที่มีลำดับความสําคัญ  ๗.๖ การควบคุมอุปกรณสื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองคกร (Mobile computing and teleworking)  ๗.๖.๑ มีการปองกันอุปกรณสื่อสารประเภทพกพา  ๗.๖.๒ มีการควบคุมการปฏิบัติงานจากภายนอกหน่วยงาน  **สรุป การควบคุมการเขาถึงระบบสารสนเทศและฐานข้อมูล**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุงการควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๘. การจัดหา การพัฒนา และการบํารุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)**  **วัตถุประสงค์ของการควบคุม**  *เพื่อใหมีวิธีการที่สอดคลองและไดผลในการบริหารจัดการ เหตุการณที่เกี่ยวของกับความมั่นคงปลอดภัยสําหรับสารสนเทศขององคกร*  ๘.๑ มีการวิเคราะหและการระบุขอกําหนดทางดานความมั่นคงปลอดภัย  ๘.๒ การประมวลผลสารสนเทศในแอพพลิเคชั่น (Correct processing in applications )  ๘.๒.๑ มีการตรวจสอบขอมูลนําเขา  ๘.๒.๒ มีการตรวจสอบขอมูลที่อยูในระหวางการประมวลผล  ๘.๒.๓ มีการตรวจสอบความถูกตองของข้อความ  ๘.๒.๔ มีการตรวจสอบขอมูลนําออก  ๘.๓ มาตรการการเขารหัสขอมูล (Cryptographic controls)  ๘.๓.๑ มีมาตรการการใชงานการเขารหัสขอมูล  ๘.๓.๒ มีการบริหารจัดการกุญแจเขารหัสขอมูล  ๘.๔ การสรางความมั่นคงปลอดภัยใหกับไฟลของระบบที่ใหบริการ (Security of system files)  ๘.๔.๑ มีการควบคุมการติดตั้งซอฟตแวรลงไปยังระบบที่ใหบริการ  ๘.๔.๒ มีการปองกันขอมูลที่ใชสําหรับการทดสอบ  ๘.๔.๓ มีการควบคุมการเขาถึง source code สําหรับระบบ  ๘.๕ การสรางความมั่นคงปลอดภัยสําหรับกระบวนการในการพัฒนาระบบและ กระบวนการสนับสนุน (Security in development and support processes)  ๘.๕.๑. มีขั้นตอนปฏิบัติสําหรับควบคุมการเปลี่ยนแปลงหรือแกไขระบบ  ๘.๕.๒. มีการตรวจสอบการทํางานของแอพพลิเคชั่นภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ  ๘.๕.๓ มีการจํากัดการเปลี่ยนแปลงแกไขซอฟตแวรที่มาจากผูผลิต  ๘.๕.๔ มีการปองกันการรั่วไหลของสารสนเทศ  ๘.๕.๕ มีการพัฒนาซอฟตแวรโดยหนวยงานภายนอก  ๘.๖ มีมาตรการการบริหารจัดการชองโหวในฮารดแวรและซอฟตแวร (Technical Vulnerability Management)  **สรุป**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุงการควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๙. การบริหารจัดการเหตุการณที่เกี่ยวของกับความมั่นคงปลอดภัยของหน่วยงาน**  **วัตถุประสงค์ของการควบคุม**  *เพื่อใหเหตุการณและจุดออนที่เกี่ยวของกับความมั่นคง ปลอดภัย ตอระบบสารสนเทศขององคกรไดรับการดําเนินการที่*  *ถูกตองในชวงระยะเวลาที่เหมาะสม*  ๙.๑ การรายงานเหตุการณและจุดออนที่เกี่ยวของกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)  ๙.๑.๑ มีการรายงานเหตุการณที่เกี่ยวของกับความมั่นคงปลอดภัย  ๙.๑.๒ มีการรายงานจุดออนที่เกี่ยวของกับความมั่นคงปลอดภัยของหน่วยงาน  ๙.๒ การบริหารจัดการและการปรับปรุงแกไขตอเหตุการณที่เกี่ยวของกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)  ๙.๒.๑ มีการกำหนดหนาที่ความรับผิดชอบและขั้นตอนการปฏิบัติ  ๙.๒.๒ มีการเรียนรูจากเหตุการณที่เกี่ยวของกับความมั่นคงปลอดภัย  ๙.๒.๓ มีการเก็บรวบรวมหลักฐาน  **สรุป**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุงการควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๑๐. การบริหารความตอเนื่องในการดําเนินงานของหน่วยงาน**  **วัตถุประสงค์ของการควบคุม**  *เพื่อปองกันการติดขัดหรือการหยุดชะงักของกิจกรรมตางๆ อันเปนผลมาจากการลมเหลว หรือหายนะที่มีตอระบบสารสนเทศ และเพื่อใหสามารถกูระบบกลับคืนมาไดภายใน ระยะเวลาอันเหมาะสม*  ๑๐.๑ มีกระบวนการในการสรางความต่อเนื่องใหกับการปฏิบัติราชการ  ๑๐.๒ มีการประเมินความเสี่ยงในการสรางความตอเนื่องใหกับการปฏิบัติราชการ  ๑๐.๓ มีการจัดทําและใชงานแผนสรางความต่อเนื่องใหกับการปฏิบัติราชการ  ๑๐.๔ มีการกําหนดกรอบสําหรับการวางแผนเพื่อสรางความ ตอเนื่องใหกับการปฏิบัติราชการ  ๑๐.๕ มีการทดสอบและการปรับปรุงแผนสร้างความตอเนื่องใหกับการปฏิบัติราชการ  **สรุป**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุงการควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................**๑๑. การปฏิบัติตามขอกําหนดทางกฎหมาย**  วัตถุประสงค์ของการควบคุม  เพื่อหลีกเลี่ยงการละเมิดขอกําหนดทางกฎหมายระเบียบปฏิบัติขอกําหนดในสัญญาและขอกําหนดทางดานความมั่นคงปลอดภัยอื่นๆ  ๑๑.๑ มีการระบุขอกําหนดตางๆ ที่มีผลทางกฎหมาย  ๑๑.๒ มีการปองกันสิทธิและทรัพยสินทางปัญญา  ๑๑.๓ มีการปองกันขอมูลสําคัญที่เกี่ยวของกับหน่วยงาน ๑๑.๔ มีการปองกันขอมูลสวนตัว  ๑๑.๕ มีการปองกันการใชงานอุปกรณประมวลผลสารสนเทศ ผิดวัตถุประสงค์  ๑๑.๖ มีการใชงานมาตรการการเขารหัสขอมูลตามขอกําหนด  **สรุป**  *การควบคุมเพียงพอ กรณีไม่เพียงพอมีแนวทางหรือวิธีการปรับปรุงการควบคุมภายใน ให้ดีขึ้น*ดังนี้..........................................................  ........................................................................................................  **๑๒. อื่นๆ** |  |  |  |

**สรุป :**

ชื่อผู้ประเมิน

ตำแหน่ง

วันที่ / /

หมายเหตุ **การใช้แบบสอบถาม**

๑. ผู้ประเมินเป็นผู้ถามตามแบบสอบถาม **ถ้ามีการปฏิบัติตามคำถามแสดงถึงการควบคุมภายในที่ดีให้กรอกเครื่องหมาย “√”** **ในช่อง “มี/ใช่”** **ถ้าไม่มีการปฏิบัติตามที่ถามให้กรอกเครื่องหมาย “x” ในช่อง “ไม่มี/ไม่ใช่” ถ้าไม่มีกิจกรรมที่เกี่ยวกับเรื่องที่ถามให้กรอกในช่อง “ไม่มี/ไม่ใช่” โดยใช้อักษร NA ซึ่งย่อมาจาก Not Applicable และหมายเหตุว่า ไม่มีเรื่องที่เกี่ยวกับคำถาม**

๒. คำตอบว่า “ไม่มี/ไม่ใช่” หมายถึง มิได้ปฏิบัติตามคำถาม แสดงถึงจุดอ่อนของระบบการควบคุมภายใน ผู้ประเมินควรทดสอบและหาสาเหตุ และพิจารณาว่ามีการควบคุมอื่นทดแทนหรือไม่จากคำตอบที่ได้รับผู้สอบทานหรือผู้ประเมินควรสังเกตการณ์การปฏิบัติงานจริง การวิเคราะห์เอกสารหลักฐาน หรือคำตอบของผู้ที่มีความรู้ในเรื่องที่ถามและเชื่อถือได้ เพื่อสรุปคำตอบและอธิบายวิธีปฏิบัติในแต่ละข้อของคำถามในช่อง “คำอธิบาย/คำตอบ” เพื่อให้ได้ข้อมูลที่ถูกต้องที่จะนำมาประเมินความเพียงพอของระบบการควบคุมภายใน

๓. จากข้อมูลในช่อง “อธิบาย/คำตอบ” จะนำมาพิจารณาประเมินความเพียงพอของระบบการควบคุมภายในของแต่ละด้านและแต่ละเรื่องในด้านนั้นๆ