# บทคัดย่อ


**ชื่อเรื่อง** : แนวทางการพัฒนามาตรการป้องกันระบบสารสนเทศ กองบัญชาการกองทัพไทย

**โดย** : พันเอก ยิ่งโรจน์ สันติวุฒน์

**อาจารย์ที่ปรึกษาเอกสารวิจัย** : **นาวาอากาศเอก**

**(ธานี สวัสดี )**

**กรกฎาคม ๒๕๖๕**

ภัยคุกคามทางไซเบอร์สามารถเริ่มต้นขึ้นจากช่องโหว่เล็กๆของทรัพย์สินสารสนเทศและกระจายความเสียหายต่อไปยังส่วนอื่นๆจนความเสียหายเกิดขยายวงกว้างขัดขวางการดำเนินกิจกรรมสำคัญของประเทศได้ ดังนั้นเพื่อเป็นการความรับผิดชอบต่อส่วนรวม พระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.๒๕๖๒ จึงได้ออกข้อบังคับให้หน่วยงานรัฐและภาคส่วนที่ให้บริการสำคัญต้องมีการออกมาตรการป้องกันระบบสารสนเทศเพื่อปิดกั้นช่องโหว่ของระบบสารสนเทศภายในองค์กรให้เป็นไปตามมาตรฐานป้องกันไม่ให้เกิดถูกโจมตีและขยายตัวออกไปเกิดความเสียหายกับสาธารณะกลายเป็นอุปสรรคสำคัญต่อการขับเคลื่อนและพัฒนาประเทศ งานวิจัยนี้ได้ศึกษาแนวทางการใช้มาตรการควบคุมในการปกป้องระบบสารสนเทศกองบัญชาการกองทัพไทยเพื่อหาปัญหาและปัจจัยที่สามารถนำมาใช้เพื่อปรับปรุงประสิทธิภาพในการกำหนดมาตรการควบคุมในการป้องกันระบบสารสนเทศให้ดียิ่งขึ้นโดยการศึกษาระบบความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 ซึ่งมีการพัฒนาและใช้งานมาอย่างกว้างขวางยาวนานและเปรียบเทียบกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. ซึ่งพัฒนาตามแนวทาง NIST Cyber Security Framework

จากการเปรียบเทียบแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ บก.ทท. และระบบความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2013 พบว่ามีปัจจัยสำคัญ ๒ ประเด็นที่มีความเป็นไปได้ที่จะนำมาใช้แนวทางพัฒนาปรับปรุงการใช้มาตรการควบคุมในการปกป้องระบบสารสนเทศกองบัญชาการกองทัพไทยคือ การกำหนดขอบเขตรายการทรัพย์สินสารสนเทศทั้งหมดในระบบสารสนเทศอย่างครบถ้วนสมบูรณ์ และการประเมินความเสี่ยงของรายการทรัพย์สินสารสนเทศแต่ละรายการก่อนแล้วจึงเลือกมาตรการควบคุมตามผลการประเมินความเสี่ยงให้เหมาะสมกับความเสี่ยงของรายการทรัพย์สินนั้นๆ แล้วจึงนำปัจจัยสำคัญ ๒ ประเด็นไปทำการสัมภาษณ์ความคิดเห็นจากผู้เชี่ยวชาญที่ปฏิบัติงานเกี่ยวกับความปลอดภัยของระบบสารสนเทศกองบัญชาการกองทัพไทยทั้งระดับ

ผู้บริหารและเจ้าหน้าที่เทคนิคซึ่งทุกท่านเห็นตรงกันว่าแนวทางการกำหนดขอบเขตรายการทรัพย์สินสารสนเทศให้ครบถ้วนสมบูรณ์มีความจำเป็นในการปกป้องระบบสารสนเทศให้ปลอดภัยและมีการให้ความเห็นเพิ่มเติมเกี่ยวกับการใช้มาตรการควบคุมตามความสำคัญของทรัพย์สินแม้จะอาจไม่ได้มาตรการควบคุมที่เหมาะสมกับความเสี่ยงของรายการทรัพย์สินแต่ละรายการเพราะไม่ได้ประเมินความเสี่ยงก่อนเลือกมาตรการควบคุมแต่สามารถทำได้ง่ายและรวดเร็วกว่าเหมาะกับการวางมาตรการควบคุมขั้นต้นและสามารถจัดลำดับความสำคัญของทรัพย์สินที่ต้องรีบดำเนินการก่อน

แนวทางในการดำเนินการพัฒนามาตรการควบคุมในการปกป้องระบบสารสนเทศกองบัญชาการกองทัพไทยมีต้องการมีบัญชีระบุรายการทรัพย์สินสารสนเทศในระบบสารสนเทศที่ครบถ้วนสมบูรณ์ส่วนการเลือกใช้มาตรการควบคุมในการปกป้องระบบสารสนเทศอาจเริ่มต้นตามความสำคัญของทรัพย์สินแล้วจึงการประเมินความเสี่ยงทรัพย์สินของสารสนเทศเพื่อปรับมาตรการควบคุมตามผลการประเมินความเสี่ยงให้ตรงกับความเสี่ยงของรายการทรัพย์สินนั้นๆเพื่อลดการสิ้นเปลืองงบประมาณ กำลังพล และการใช้ระบบสารสนเทศที่ยุ่งยากที่ไม่จำเป็นออกไป

# Abstract

**TITLE** : An Approach to Improve Security Controls for Information System of Royal Thai Armed Forces Headquarter

**By** : Col. Yingrodge Suntiwuth

**Research Advisor** : **Group Captain**

**( Thanee Sawasdee )**

**July 2022**

Cyber threats can begin from a small crack in an information asset and spread the damage to the rest of the world until the damage can be widespread, impeding the operations of a country's vital activities. Therefore, in order to be responsible for the public, the Cybersecurity Act B.E. 2562 has stipulated that government agencies and key service sectors must issue control measures to protect vulnerabilities in their information systems, preventing them from being attacked and spreading damages to public. This research examines the guideline for the use of protection control measures for the Information System of the Royal Thai Armed Forces Headquarter. By comparing with the control measures establishment of protection process used by the ISO/IEC 27001:2013 standard, the two problem sfactors for improvement were identified and both factors can potentially be used to improve the process for the information systems of the Royal Thai Armed Forces Headquarter to establish the protection control measures process.

The two factors which are likely to be adopted for improvements in the use of protection control measures of the Royal Thai Armed Forces Information System are: 1) the completeness of the scope of information assets in the information system and 2) the conduct of risk assessment before selecting control measures to match risks of the information asset. Then both factors became the issues for interviewing experts who are working on information systems security area of the Royal Thai Army Headquarters in both at the executive and technical levels. All of them agree that the completeness of the scope of information assets is very important in safeguarding the information

system. Moreover, some shared an important opinion on the use of impact-based control measures that the method are easier and faster and is suitable for initial determining of control measures because this method can prioritize assets that require immediate action.

An approach for the development of control measures to protect information systems of the Royal Thai Armed Forces Headquarters are: first, defining list of complete information assets of the information system and; second, selecting of control measures according to the risk assessment results. The control measures to protect information systems may begin according to the asset importance, however, risk assessment should be conducted as soon as possible in order to adjust the control measures to match accordingly with asset risks to reduce the wasted budget, manpower, and the unnecessary use of complicated information systems.