Thaioil 2025 Information Security Management Programs

Updated: June 2026

2025 Information Security Management Programs

The landscape of information security threats is constantly expanding and adapting, using both emerging and established technologies to target weaknesses. To safeguard systems and sensitive data, and effectively address these threats, Thaioil has implemented information security management programs aimed at testing and securing their information systems.

Key Performance in 2025

1 External Audit for Re-Assessment ISO27001 certification of all IT infrastructure and Information Security Management with non-conformities and no observation

2 Internal audit for OT cyber and Digital Project Management

2 cyber drill table top exercise for information security-related business continuity plans were conducted.

100% of Phishing test exercise for all employees, spear phishing for management

100% information security/cybersecurity awareness training for new employees and Administrators

Engaging Cyber Insurance program to cover incident response services with cyber experts

Zero cases of Cyber Attack & information security breaches.

Source: https://www.thaioilgroup.com/en/sustainability/governance-and-economics-dimension-digital-management/

2025 Information Security Management Programs

External Audits of the IT Infrastructre and Information Security Management Sydtems

ISO/IEC 27001

Certificate of Approval
This is to certify that

Thai Oil Public Company Limited

Address of head office : 555/1 Energy Complex, Building A, 11th Floor, Vibhavadi Rangsit Road, Chatuchak, Chatuchak District, Bangkok 10900, Thailand

has been assessed and found to be conforming to the requirements of ISO/IEC 27001:2013 include ISO/IEC 27001:2013/cor2:2015 Information Security Management System

for the scope :

The computer data center management and application software services of SAP system, LIMS systems, Advanced Process Control Networks, Instrument networks, Electrical Integrated control system (ELICS), Telecommunication network and storage CCTV system.
This is in accordance with the Statement of Applicability (SoA) Version 4.1 dated 21.09.2021

By Management System Certification Institute (Thailand), Foundation for Industrial Development

Date of Issue 4th December 2022
Valid Until 3rd December 2025
First Issued Date 4th December 2019

(Mr. Jongrak Rojpalasatean)
President
Management System Certification Institute (Thailand)

MASCI

Page 1/3

Thaioil has successfully completed ISO27001 re-assessment programs. This certification covers 100% of organization critical Information Technology and Operation Technology as follow:

- The Data Center, SAP, and LIMS systems, under the control and management of the Digital Function.
- Advanced Process Control Network, under the control and management of the Technology Process Control Function, which supports service activities and work processes within the Thaioil Group.
- Instrument Network, under the control and management of the Instrument Engineering Functions.
- Telecommunication and ELICS systems, under the control and management of the Electrical Engineering functions.

Year 2025 Re-assessment Results

Zero (0) Non-Conformities: Full adherence to all regulatory and ISO standards.
Zero (0) Observations: Complete alignment with best practices e.g. NIST Framework.

See more: https://thaioilwebsite.s3.ap-southeast-1.amazonaws.com/wp-content/uploads/2024/09/24082905/ISO27001-Eng.pdf

2025 Information Security Management Programs

Internal Audits of the IT Infrastructure and Information Security Management Systems

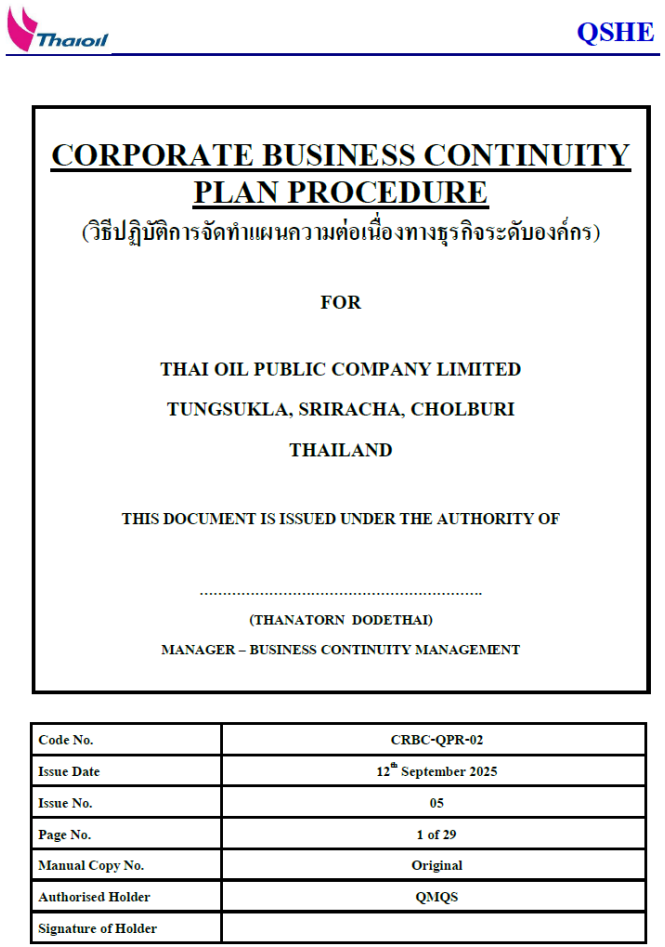
Year 2025 Results , Thaioil formulated and conducted 2 cybersecurity audit work plan. The scope of the audit work plan as followed:

- Operational Technology (OT) Cybersecurity
- Digital Project Management"

See more: https://thaioilwebsite.s3.ap-southeast-1.amazonaws.com/wp-content/uploads/2024/09/24082905/ISO27001-Eng.pdf

2025 Information Security Management Programs

Information security-related business continuity plans



Thaioil QSHE

CORPORATE BUSINESS CONTINUITY PLAN PROCEDURE

(วิธีปฏิบัติการจัดทำแผนความต่อเนื่องทางธุรกิจระดับองค์กร)

FOR

THAI OIL PUBLIC COMPANY LIMITED

TUNGSUKLA, SRIRACHA, CHOLBURI

THAILAND

THIS DOCUMENT IS ISSUED UNDER THE AUTHORITY OF

.....

(THANATORN DODETHAI)

MANAGER – BUSINESS CONTINUITY MANAGEMENT

Code No.	CRBC-QPR-02
Issue Date	12th September 2025
Issue No.	05
Page No.	1 of 29
Manual Copy No.	Original
Authorised Holder	QMQS
Signature of Holder	

Thaioil awares that information security incidents may result in significant business disruption. Accordingly, information security factor has been incorporated into Thaioil's Business Continuity Management (BCM) framework and Business Continuity Plans (BCP) consideration, as addressed in environmental scanning and risk assessment section of Corporate Business Continuity Plan Procedure.

BCM framework comprehensively addresses potential impacts on information assets, technology infrastructure, systems, and data arising from various disruption scenarios, including but not limited to:

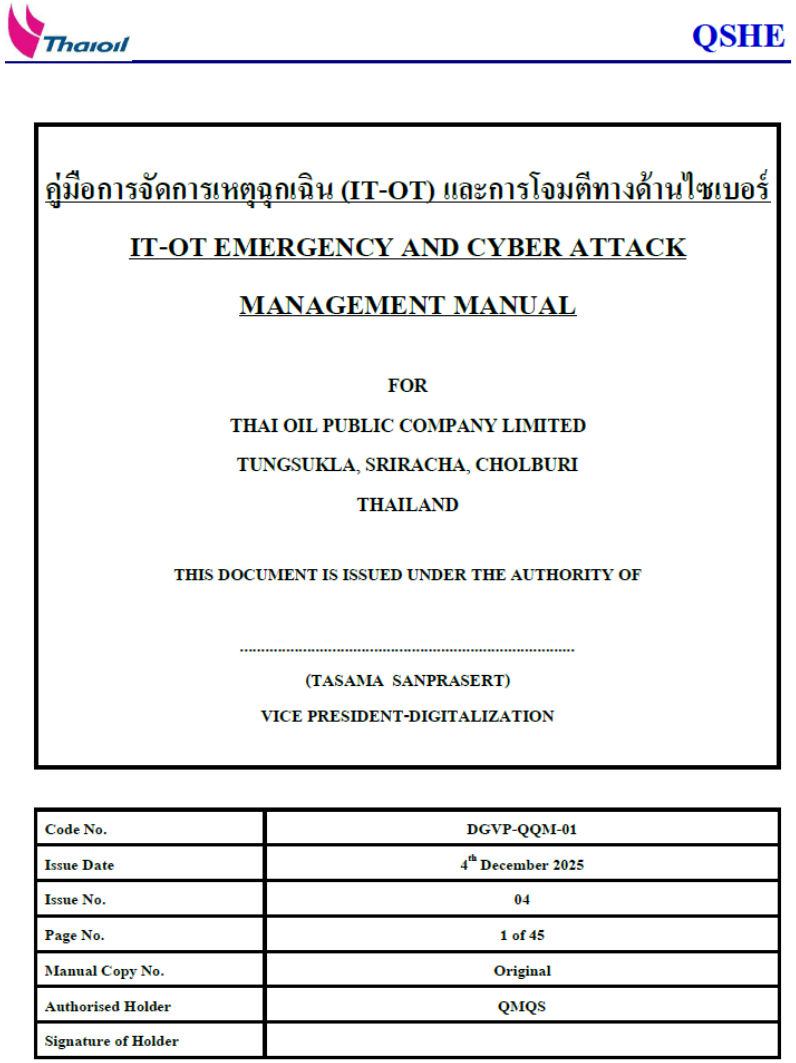
- Cyberattacks and IT system failures
- Failures of critical systems, including IT systems, databases, emergency response systems, BCM systems, and permit-related systems
- Outdated or inadequate information security policies, procedures, and guidelines
- Cyber threats involving unauthorized access attempts by hackers or malicious actors
- Cyber ransomware incidents

BCP also defines the roles and responsibilities of relevant departments and response teams, operating under the direct oversight of the Chief Executive Officer (CEO), management executives, and other responsible personnel involved in BCM process.

For Year 2025, to ensure Thaioil can protect, sustain, and recover its critical operations during disruptions or security incidents, BCP supports DG team on cyber security drill of PI system attack.

2025 Information Security Management Programs

Information Security Incident Response



Thaioil QSHE

คู่มือการจัดการเหตุฉุกเฉิน (IT-OT) และการโจมตีทางด้านไซเบอร์

IT-OT EMERGENCY AND CYBER ATTACK

MANAGEMENT MANUAL

FOR

THAI OIL PUBLIC COMPANY LIMITED

TUNGSUKLA, SRIRACHA, CHOLBURI

THAILAND

THIS DOCUMENT IS ISSUED UNDER THE AUTHORITY OF

.....

(TASAMA SANPRASERT)

VICE PRESIDENT-DIGITALIZATION

Code No.	DGVP-QQM-01
Issue Date	4th December 2025
Issue No.	04
Page No.	1 of 45
Manual Copy No.	Original
Authorised Holder	QMQS
Signature of Holder	

Thaioil has its IT-OT Emergency and Cyber-attack management manual as a guide for handling emergency situations from cyber-attack that may affect the company's Information System. The document addresses **escalation process for employees to report incidents, vulnerabilities or suspicious activities** relating to information security.

The content of this document includes;

- Contact number and operational center in emergency case
- Organization management in emergency case
- Roles and responsibilities structures
- Procedure and workflow in case of emergency
- Overall incident escalation flow
- Initial Incident Management
- Emergency Management
- Recovery and Return to Usual Circumstances

The document describes Thaioil's organizational structure for effective cyber-attack management and emergency management including a list of people involved and their roles and responsibilities. This is for everyone involved in emergency management and cyberattack management. Also, it illustrates the responsibility of the Cyber Emergency Response Team (CERT) who oversees Thaioil's cybersecurity and IT security and the highest responsibility position of CERT (CERT Commander, EVPN whose position is equivalent to CISO)

Year 2025 Results, Thaioil collaborated with specialized consultants and executive leadership to review and execute a comprehensive Cybersecurity Tabletop Exercise Plan. Through the execution of two separate tabletop exercises, the organization effectively validated its incident response protocols and significantly enhanced the executive team's incident readiness.

2025 Information Security Management Programs

Information Security Testing by Vulnerability and Penetration testing activities

Year 2025 Results, To ensure a robust and continuous level of security protection, company maintained its standard cybersecurity controls which included

- Vulnerability Management: Conducted comprehensive vulnerability scanning and technical analysis on a quarterly basis.
- Identity & Access Management (IAM): Completed a 100% comprehensive review of all standard user accounts and privileged access accounts to enforce the principle of least privilege.
- Supply Chain Security: Executed formal third-party risk assessments for all IT major vendors.
- Real World Attack Simulation : Executed Penetration and Red Teaming Simulation with external parties.

2025 Information Security Management Programs

CyberSecurity Awareness and Phishing Test Exercise

Thaioil aims to empower individuals within an organization to become the first line of defense against cyber threats.

Year 2025 results, Thaioil completed the cybersecurity awareness activities by

- 100% of new employee during on-boarding process
- 100% of IT administrators
- Completed 4 phishing test simulation for all staffs and 1 spear phishing
- 100% of direct communication employees who fell victims by line manager