GPSC

Information Security Management Program 2025

Content

Introduction

In today’s fast-evolving digital landscape, the protection of information assets is essential to maintaining business continuity, operational efficiency, and stakeholder trust. Recognizing the increasing complexity of cyber threats and the critical importance of safeguarding data, the company has established a comprehensive Information Security Management Program to guide its approach to information protection, risk mitigation, and regulatory compliance. The Information security management program provides a structured framework for identifying, assessing, and managing information security risks across all business units and functions. It aligns with international standards and best practices, promoting a consistent and proactive security culture throughout the organization. The program emphasizes not only technical controls but also governance, policies, awareness, and the continuous improvement of systems and processes. Through this program, the company aims to ensure the confidentiality, integrity, and availability of its information assets while supporting secure business operations, protecting stakeholder interests, and enabling sustainable digital growth.

Information security-related business continuity plans

Information security-related business continuity plans

GPSC has the business continuity plan (BCP) as practical approach in recovery the main operation of GPSC (Announced on 1 Feb 2025). The plan has included the incident response related to business continuity plan (BCP) of GPSC that covers IT System/Network Failure and cyber attack, the structure of management team associated with the incident, role and relevant department, the process of implementation, and the recovery plan from the incidents.

Objective

- Define the framework for the organization's business continuity management during a crisis situation.
- Establish the structure of crisis management teams and related working groups, including clearly defined roles and responsibilities for each group.
- Outline the procedures to be followed in response to a crisis event. Specify the actions to be taken when the Business Continuity Plan (BCP) is activated.
- Provide definitions and terminology to ensure a shared and accurate understanding

Scope

This plan has been established for GPSC to serve as a guideline for action in the event that the BCP is triggered to activate. All personnel within the business unit are expected to adhere to the procedures outlined in this plan, as well as those detailed in the unit-specific BCP. Employees who have been assigned designated roles, whether in the Primary Response Team or the Backup Response Team, are responsible for performing the tasks associated with their roles, as specified in both this plan and the relevant unit's continuity plan. The scenarios that are the key disaster for plan activation constitute production interruption, delivery interruption, office deny, and IT System/ Network failure.

Business continuity plan (BCP)

GPSC Group
Work Instruction
ชื่อเอกสาร: แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)
หมายเลขเอกสาร: PDV-WI-0030

หน้า 1 of 13
ครั้งที่แก้ไข 02
วันที่ประกาศ 1 กุมภาพันธ์ 2568

GPSC
Global Power Synergy Public Company Limited

วิธีปฏิบัติงาน
Work Instruction

ข้อมูลเอกสารฉบับล่าสุด

หมายเลขเอกสาร	PDV-WI-0030	Business Unit (Function)	PSE	Dep/Div.	PDV
ชื่อเอกสาร	แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan)			สถานะ	ประกาศใช้
Revision	02	วันที่ประกาศใช้	1 กุมภาพันธ์ 2568	จำนวนหน้า	13
ตำแหน่งที่จัดเก็บไฟล์เอกสาร	GPSC Corporate Document Management System (CDMS) / PDV / Work Instruction				

ระบบมาตรฐานที่อ้างอิง / มาตรฐานและข้อกำหนดที่เกี่ยวข้อง

ที่	ระบบ / มาตรฐาน	ข้อกำหนด
1	ISO 22301 ระบบบริหารความต่อเนื่องทางธุรกิจ	ทุกข้อกำหนด

Information security-related business continuity plans

As part of GPSC's Business Continuity Plan, the information security component includes scenario-based planning to address critical threats such as IT system or network failures and cyberattacks. These events are identified as key triggers for activating the continuity plan. In response, the plan outlines detailed, step-by-step procedures to guide the recovery process, ensuring that business operations can be restored efficiently and effectively in the event of a disruption. This approach enhances organizational resilience and preparedness against information security incidents.

สถานการณ์หลัก (Key Scenarios)	สถานการณ์ย่อย (Sub Scenarios)
1. การหยุดชะงักของกระบวนการผลิต (Production interruption)	Confidential
2. การหยุดชะงักของการส่งมอบผลิตภัณฑ์ (Delivery interruption)	
3. ไม่สามารถเข้าปฏิบัติงานในสถานที่ (Office Deny)	
4. ระบบเทคโนโลยีสารสนเทศไม่สามารถใช้งาน (IT System/Network Failure)	4.1 โจมตีทางไซเบอร์ (Cyber Attack)

ลำดับ	แผนปฏิบัติงาน	ผู้รับผิดชอบ
1.	เตรียมความพร้อมคอมพิวเตอร์ – จัดหาเครื่องคอมพิวเตอร์สำหรับพนักงาน และ ติดตั้งระบบ Remote Support และ ระบบ Conference ในคอมพิวเตอร์พนักงาน	Confidential
2.	เตรียมความพร้อมสำหรับการทำงานระยะไกล - ติดตั้งระบบ VPN ในคอมพิวเตอร์พนักงาน	
3.	เฝ้าระวังการโจมตีทางไซเบอร์ผ่านระบบ CSOC โดยผู้ให้บริการ PTT Digital	
4.	เตรียมความพร้อมแก้ไขระบบ Network ด้วยกระบวนการ Incident Management	
5.	เตรียมความพร้อมของ DR-Site และมี DR-Drill ของระบบต่าง ๆ ประจำปี	
6.	เตรียมความพร้อมแผนรับมือการโจมตีทางไซเบอร์ของระบบ IT โดยการทำ Cyber Drill ประจำปี	
7.	เตรียมความพร้อมแผนรับมือการโจมตีทางไซเบอร์ของระบบ OT โดยการทำ Cyber Drill ประจำปี ร่วมกับตัวแทนของโรงงาน	

Information security vulnerability analysis

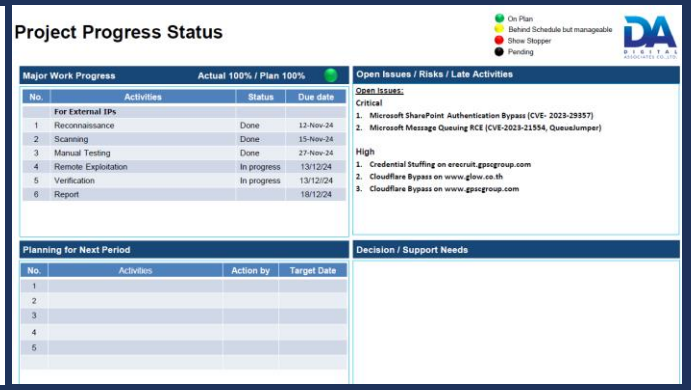
Information security vulnerability analysis (1/4)

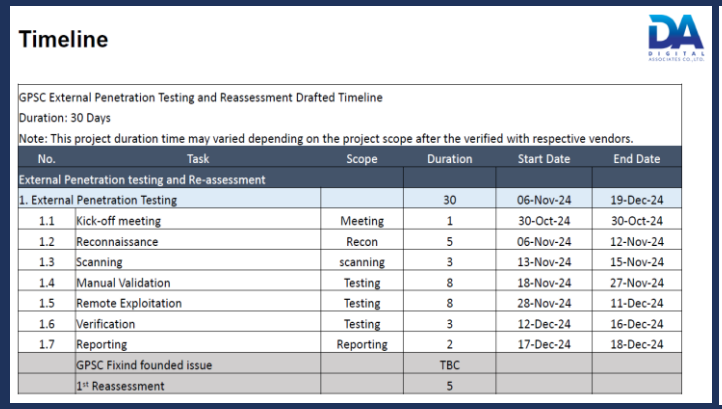
In 2024, GPSC carried out an external audit, including a comprehensive vulnerability assessment and penetration testing, to identify and address potential weaknesses in its digital systems. The evaluation was conducted by specialized cybersecurity firm (DA Digital Associates Co., Ltd.) to ensure the integrity, resilience, and security of GPSC's IT infrastructure.

Assessor: DA Digital Associate Co., Ltd

Date: 06 Nov 24 to 18 Dec 24

Result:
The assessment resulted in two different level of status, including critical and high levels of vulnerability through testing.





No.	Task	Scope	Duration	Start Date	End Date
External Penetration testing and Re-assessment					
1. External Penetration Testing			30	06-Nov-24	19-Dec-24
1.1	Kick-off meeting	Meeting	1	30-Oct-24	30-Oct-24
1.2	Reconnaissance	Recon	5	06-Nov-24	12-Nov-24
1.3	Scanning	scanning	3	13-Nov-24	15-Nov-24
1.4	Manual Validation	Testing	8	18-Nov-24	27-Nov-24
1.5	Remote Exploitation	Testing	8	28-Nov-24	11-Dec-24
1.6	Verification	Testing	3	12-Dec-24	16-Dec-24
1.7	Reporting	Reporting	2	17-Dec-24	18-Dec-24
	GPSC Fixind founded issue		TBC		
	1st Reassessment		5		

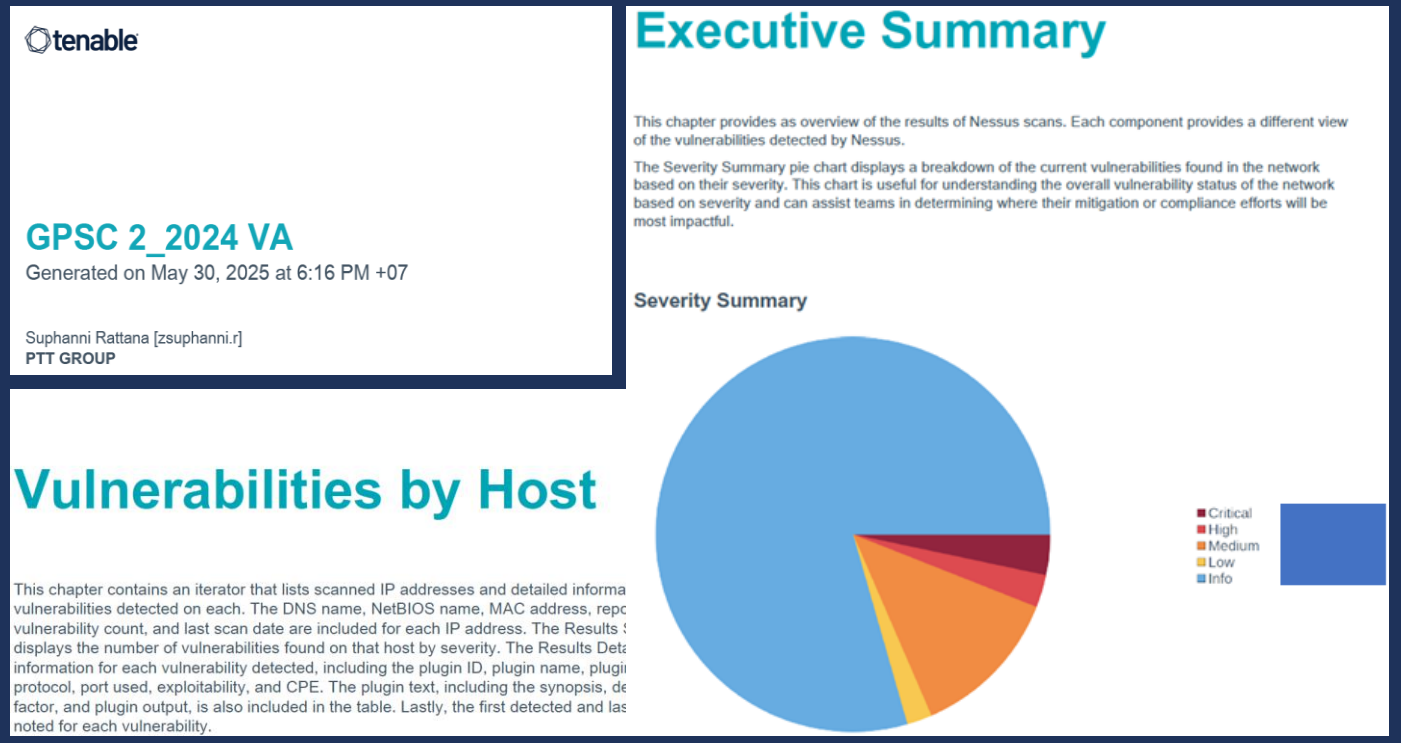
Information security vulnerability analysis (2/4)

GPSC carried out an external audit for vulnerability assessment to identify and address potential weaknesses in its digital systems. The evaluation was conducted by specialized cybersecurity firm (Tenable, Inc.) to ensure the integrity, resilience, and security of GPSC's IT infrastructure.

Assessor: Tenable, Inc.

Date: 06 Nov 24 to 18 Dec 24

Result:
The assessment resulted in five different level of status, including critical, high, medium, low, and info levels of vulnerability through testing.



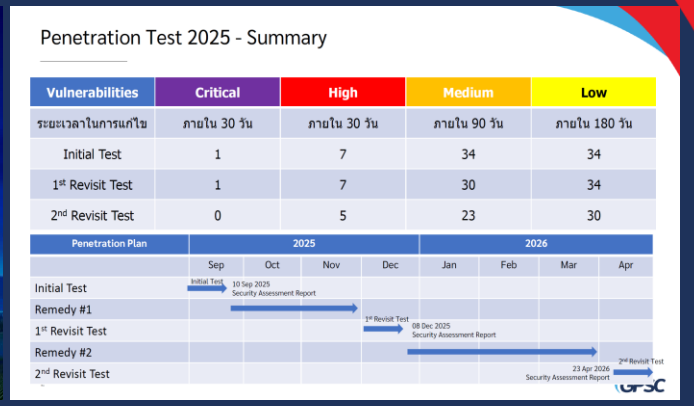
Information security vulnerability analysis (3/4)

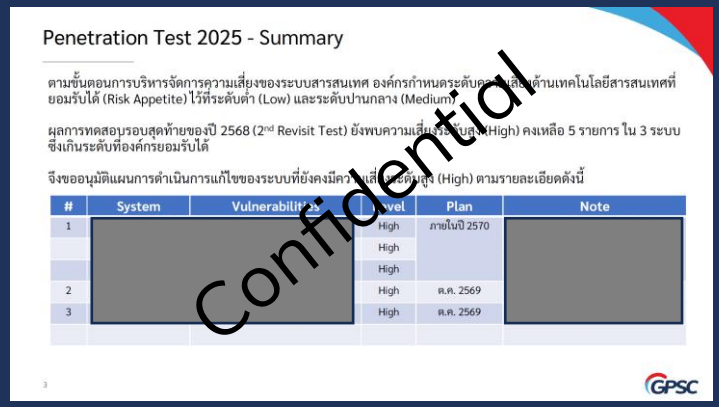
In 2025, GPSC applies a defined risk appetite (accepting only Low and Medium residual risk) and manages identified vulnerabilities through a closed-loop remediation process. Each finding is assigned on owner and a severity-based remediation timeline, and is re-tested in subsequent review rounds to verify that fixes are effective.

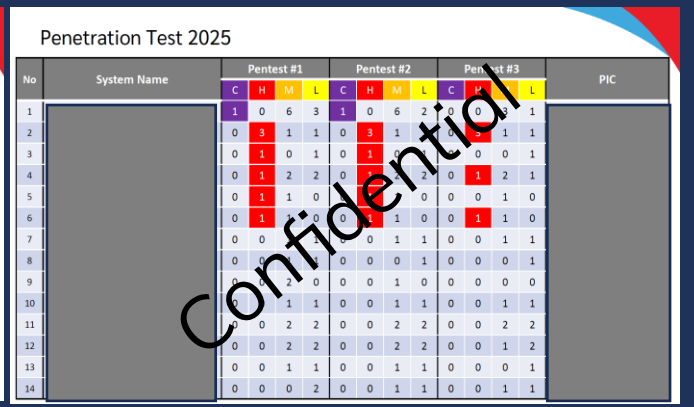
Classification : Critical / High / Medium / Low (per CVSS v3.1)

Review cycle: Initial >> 1st Revisit >> 2nd Revisit (3 rounds)

Result:
The majority of previously reported issues were remefiated across the revisit rounds; residual high-risk items are placed under a time-bound remediation plan with assigned owners.







Information security vulnerability analysis (4/4)

In 2025, GPSC carried out an external audit, including a comprehensive vulnerability assessment and penetration testing, to identify, classify and prioritize potential weaknesses in its network, application and cloud (SaaS) infrastructure. The assessment was conducted by an independent cybersecurity specialist to ensure the integrity, resilience and security of GPSC's IT infrastructure.

Assessor: TDG (independent cybersecurity specialist)

Period: 10 Sep 2025 - 23 Apr 2026 (Initial test + 2 revisit rounds)

Result:
The revisit assessment identified remaining vulnerabilities. The three high-risk findings relate to file-upload handling, broken authorization (IDOR) and unprotected web pages/APIs.

truedigital

Security Assessment Report

Revisit Penetration Testing Service

for **Global Power Synergy Public Company Limited**

23 April 2026

Penetration Testing Service for GPSC

CYBER SECURITY | truedigital

4. Finding Summary

4.1 Findings Overview

Responsible team

TDG separates the findings into 2 groups by responsible teams who need to be involved for the remediation process.

- Application-related security issues are the results of insecure programming practices and defected codes. Developer teams are normally required to rectify the discovered issues.
- Platform-related security issues are usually the results of misconfigurations or out-of-date software. Fixing these issues requires the administrator team to reconfigure, update, or remove the vulnerable software.

The following bar chart provides an overview of the vulnerabilities separated into platform-related and application-related.

Internal audits of the IT infrastructure and/or information security management systems

Internal audits of the IT infrastructure and/or information security management systems (1/6)

In 2024, GPSC conducted comprehensive internal audits to evaluate and enhance the integrity, resilience, and security of its IT infrastructure and information security management systems. These audits aimed to ensure preparedness against potential disruptions and cyber threats across the organization. Key activities included a:

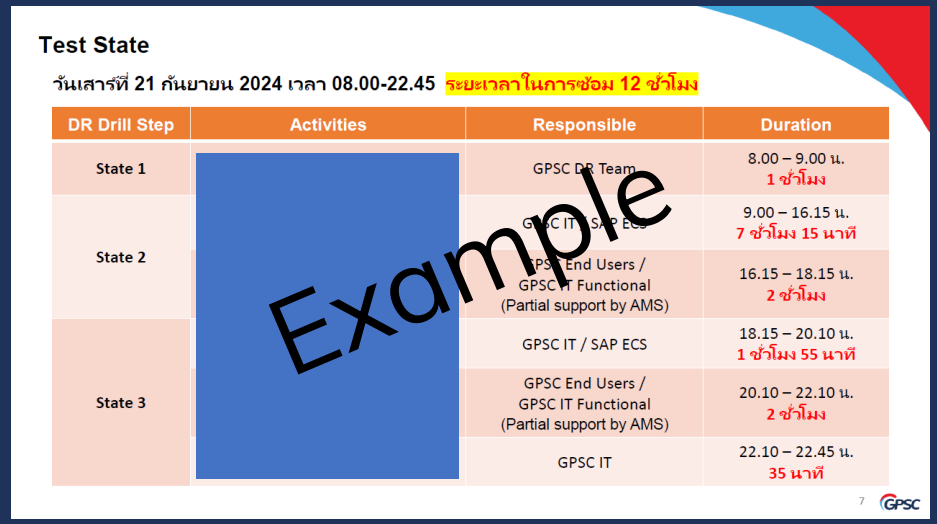
- Disaster Recovery (DR) and emergency drill for the SAP S/4 HANA system to test business continuity capabilities,
- Tabletop cyber drills focused on both operational technology (OT) and information technology (IT) systems to simulate and respond to cybersecurity incidents.
- Additionally, GPSC tested its DR plan for Cloud Infrastructure as a Service (IaaS) to validate cloud recovery protocols, and
- Carried out a phishing email simulation to assess employee awareness and response to social engineering threats.

These proactive measures reflect GPSC's commitment to maintaining a secure and resilient digital environment.

Internal audits of the IT infrastructure and/or information security management systems (2/6)

In 2024, GPSC carried out its annual Disaster Recovery (DR) and Emergency Drill for the SAP system, aiming to ensure organizational readiness in the event of an unexpected incident. The drill was designed to test the effectiveness of incident management procedures, confirm the clarity of roles and responsibilities among employees, and assess their ability to respond promptly and accurately during disruptions. In addition to evaluating the SAP S/4 HANA system, the exercise also involved critical components of GPSC's broader IT infrastructure, including servers, network configurations, storage systems, and backup environments, to ensure system interoperability and infrastructure resilience. The drill assessed the organization's Recovery Point Objective (RPO) and Recovery Time Objective (RTO) in accordance with the defined Service Level Agreement (SLA). This proactive initiative not only strengthens GPSC's operational resilience but also supports continuous improvement in business continuity and IT system recovery capabilities.

Date of internal audit: 21 Sep 2024

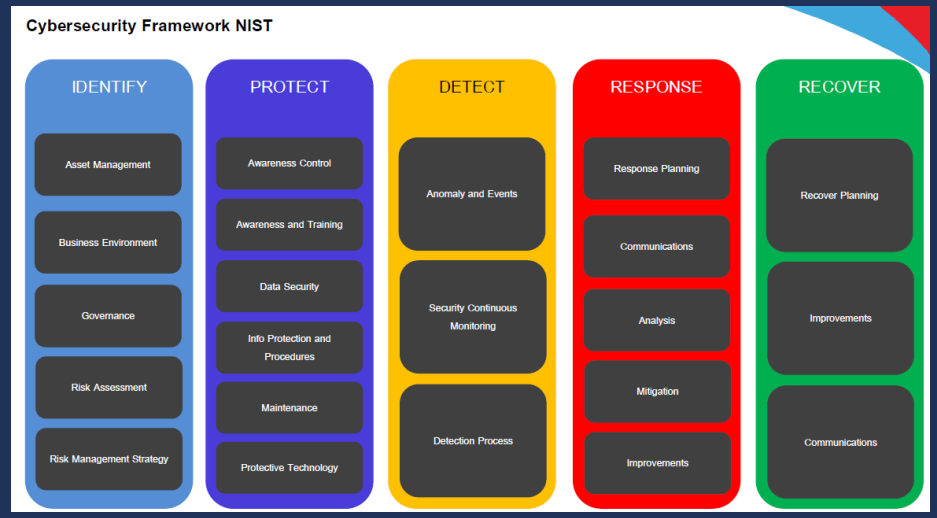


Internal audits of the IT infrastructure and/or information security management systems (3/6)

GPSC conducted cyber drill tabletop activities for operation technology and information technology in 2024 to prepare the readiness for quick incident response to recover the business operation, establish the comprehensive understanding the process for incident management for employees, and ensure role and responsibility of all employees for cyber security.

The scope of test involved a tabletop exercise combined with the activation of a command center to oversee the response. The simulation focused on handling a cybersecurity threat scenario, specifically a Zero-Day Malware Attack. Key participants in the drill included the Cyber Warfare Team (CWT), Information Security Management System (ISMS) team, Enterprise Technology Management (ETM), Plant Operation (C&I), and external service providers. The simulated attack was designed to impact critical systems such as the PI Server, PI Interface, and OPC, which in turn affected operations at CUP1, CUP4, GIPP, and Phase 5 plants. Notably, the production systems were not shut down, as the exercise was purely procedural. The entire drill was conducted online with the command center operating virtually via Microsoft Teams.

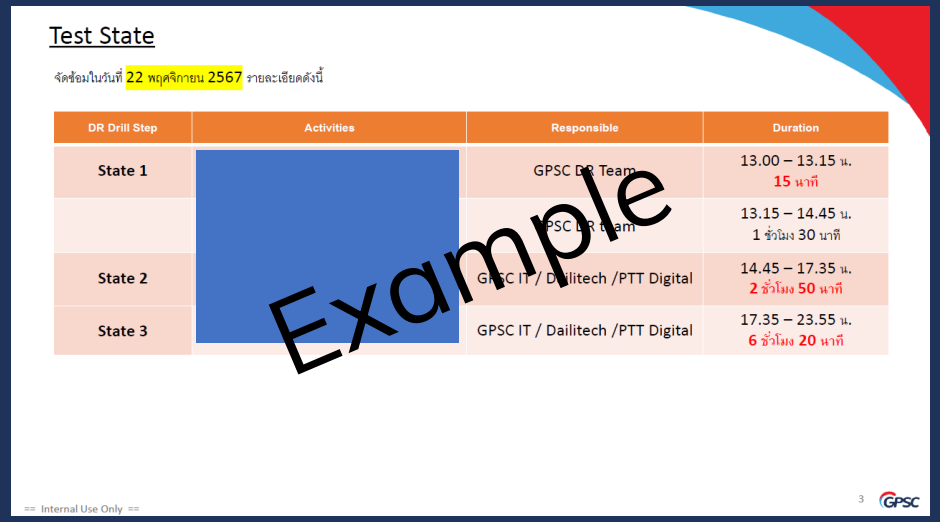
Date of internal audit: 21 Oct 2024 to 11 Dec 2024



Internal audits of the IT infrastructure and/or information security management systems (4/6)

The test focused on evaluating the organization's response to a critical incident affecting core IT infrastructure. It aimed to assess the effectiveness of emergency communication, decision-making, and coordination between internal teams and service providers. An internal audit tested the continuity of key systems and services, such as user authentication and file access, and involved declaring an emergency to ensure appropriate escalation and recovery actions were taken within the defined timeframe.

Date of internal audit: 22 Nov 2024



Internal audits of the IT infrastructure and/or information security management systems (5/6)

Phishing email simulation is one of the key internal audit programs implemented by GPSC across the organization. Conducted annually, this program serves as a practical assessment of employees' ability to recognize and respond to phishing attempts, following their participation in cybersecurity awareness training. The simulation helps evaluate the effectiveness of the training program by measuring real-time responses to potential threats, identifying areas where additional support or education may be needed, and reinforcing a culture of vigilance. This proactive approach plays a crucial role in strengthening the organization's overall cybersecurity posture and minimizing the risk of social engineering attacks.

Date of internal audit:

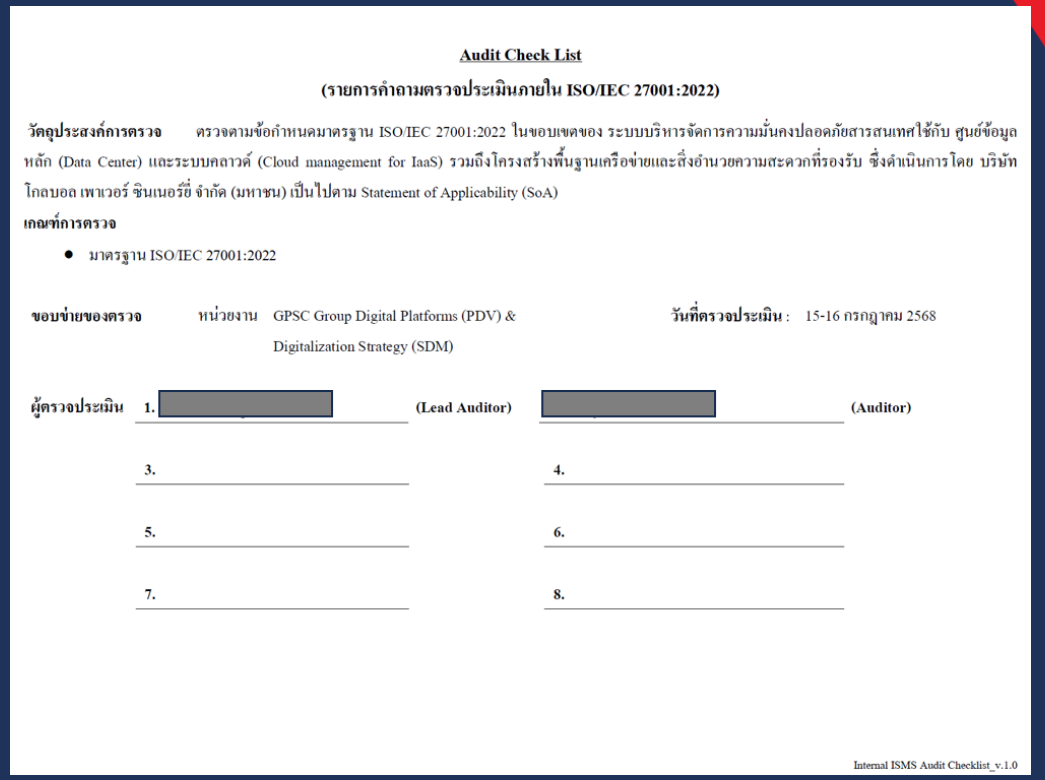
- 24 Jun 2024 to 28 Jun 2024
- 26 Aug 2024 to 30 Aug 2024

Internal audits of the IT infrastructure and/or information security management systems (6/6)

In 2025, GPSC conducts internal audits of its Information Security Management System (ISMS) against the ISO/IEC 27001:2022 standard. The most recent internal audit was carried out on 15–16 July 2025 by formally appointed independent auditors.

The audit assessed the full management-system requirements. Areas verified included information security policy and roles, technical vulnerability management, business continuity and IT disaster recovery, incident management, access control, change management, and information security awareness. Audit results are recorded against a conform / non-conformity / observation status, escalated through corrective and preventive action (CAR/PAR) tracking, and fed into management review for continual improvement.

Supporting practices confirmed during the audit include a technical vulnerability management program combining regular vulnerability scanning and annual penetration testing, with defined remediation timeframes based on severity; a documented business continuity plan supported by an ISO 22301 certification and a disaster-recovery site hosted across three availability zones; a structured information security incident management process with defined severity classifications and escalation channels; and recurring security awareness training delivered through the company's e-learning platform and new-employee onboarding.



Audit Check List

(รายการคำถามตรวจประเมินภายใน ISO/IEC 27001:2022)

วัตถุประสงค์การตรวจ ตรวจตามข้อกำหนดมาตรฐาน ISO/IEC 27001:2022 ในขอบเขตของ ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศใช้กับ ศูนย์ข้อมูลหลัก (Data Center) และระบบคลาวด์ (Cloud management for IaaS) รวมถึงโครงสร้างพื้นฐานเครือข่ายและสิ่งอำนวยความสะดวกที่รองรับ ซึ่งดำเนินการโดย บริษัท โกลบอล เพาเวอร์ ซินเนอร์ยี่ จำกัด (มหาชน) เป็นไปตาม Statement of Applicability (SoA)

เกณฑ์การตรวจ

- มาตรฐาน ISO/IEC 27001:2022

ขอบข่ายของตรวจ หน่วยงาน GPSC Group Digital Platforms (PDV) & Digitalization Strategy (SDM) **วันที่ตรวจประเมิน :** 15-16 กรกฎาคม 2568

ผู้ตรวจประเมิน 1. [redacted] **(Lead Auditor)** [redacted] **(Auditor)**

3. 4.

5. 6.

7. 8.

Internal ISMS Audit Checklist_v.1.0

Independent external audit of the IT infrastructure and/or information security management systems

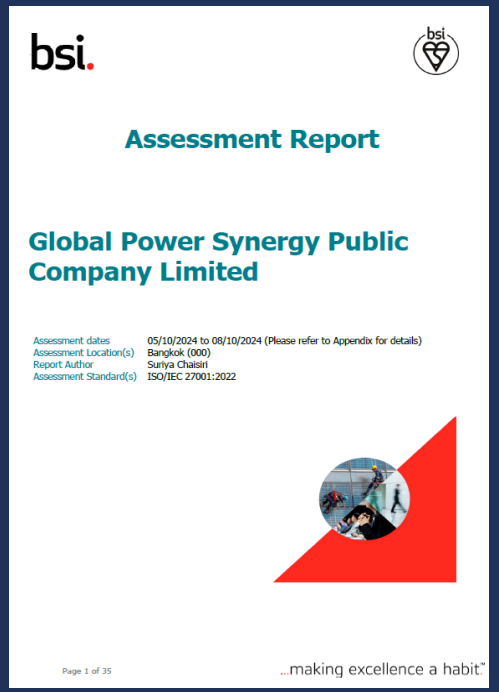
External audit of the IT infrastructure and/or information security management systems

In 2024, GPSC underwent an external audit of its IT infrastructure and information security management systems, conducted by BSI Group. As part of this process, GPSC upgraded its certification from ISO/IEC 27001:2013 to **ISO/IEC 27001:2022**. The transition reflects the organization's commitment to maintaining a robust and up-to-date information security framework. The updated 2022 version of the standard introduces a more structured approach to risk management, enhanced alignment with modern cybersecurity practices, and greater emphasis on continual improvement and stakeholder expectations. This upgrade ensures that GPSC's information security management system remains resilient, relevant, and aligned with evolving global security challenges and regulatory requirements.

Assessor: BSI Group

Assessment date: 05 Oct 2024 to 08 Oct 2024
Certificate date: 15 Nov 2024 to 14 Nov 2027

Result:
The organization has demonstrated a strong commitment to enhancing the effectiveness of its management system. Evidence shows that the system has been properly implemented and operated to achieve its intended outcomes. The management team has actively ensured compliance with internal policies, customer expectations, legal obligations, and other relevant requirements, while also fostering a culture of continual improvement. Furthermore, the organization has successfully completed the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022, reflecting its proactive approach to aligning with updated international standards.


bsi.

Assessment Report

Global Power Synergy Public Company Limited

Assessment dates	05/10/2024 to 08/10/2024 (Please refer to Appendix for details)
Assessment Location(s)	Bangkok (000)
Report Author	Suriya Chaisiri
Assessment Standard(s)	ISO/IEC 27001:2022

Page 1 of 35

...making excellence a habit.


bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2022

This is to certify that:

Global Power Synergy Public Company Limited.
555/2 Energy Complex Building B,
5th Floor, Vibhavadi- Rangsit Road,
Chatuchak, Chatuchak,
Bangkok
10900
Thailand

Holds Certificate Number: IS 752969

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2022 for the following scope:

The Information security management system applies to Data Center supporting infrastructure and cloud management (IaaS) managed by Global Power Synergy Public Company Limited in accordance with the Statement of applicability version 2.0, Date 02/09/2024

For and on behalf of BSI:

Michael Lam - Managing Director Assurance, APAC

Original Registration Date: 2021-11-15
Latest Revision Date: 2024-10-15

Effective Date: 2024-11-15
Expiry Date: 2027-11-14

Page: 1 of 2

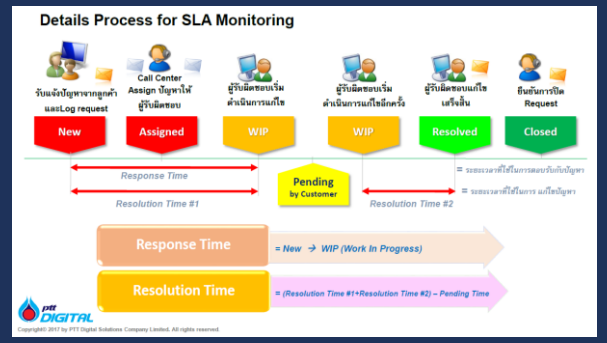
...making excellence a habit.

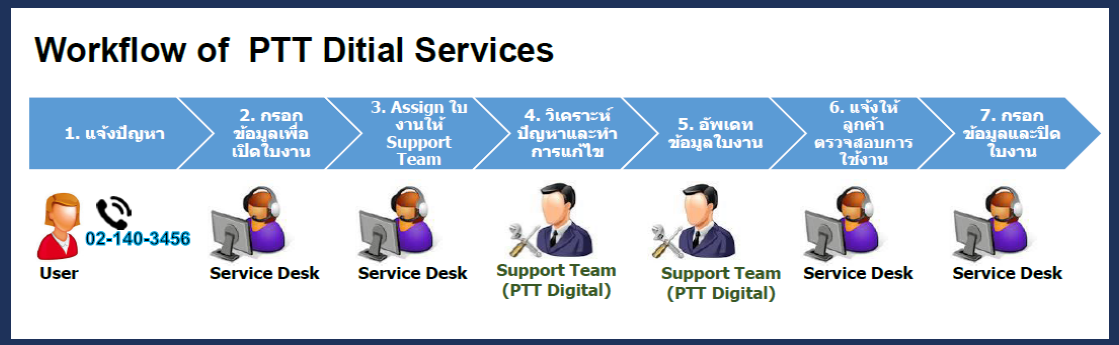
Escalation process for employees to report incidents, vulnerabilities or suspicious activities

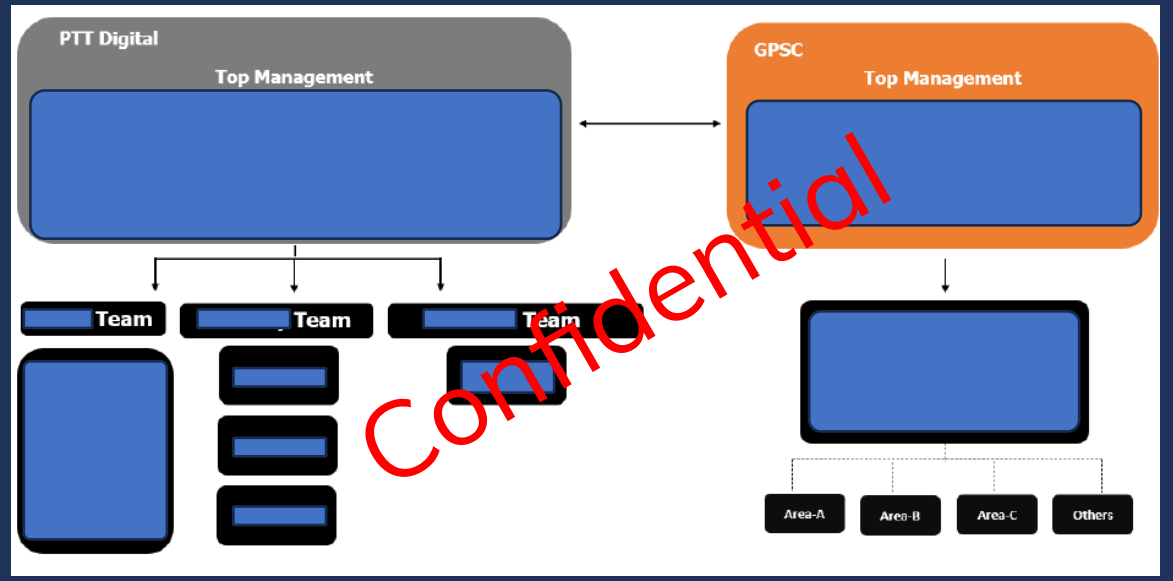
Escalation process for employees to report incidents, vulnerabilities or suspicious activities (1/3)

GPSC, as a PTT flagship company, uses the process of service level agreement (SLA) monitoring and workflow as a clear escalation process of manage information and cybersecurity event/ incident of PTT digital services as well as PTT Digital Service Request Channel for resolving the customers' IT Problems. The workflow is managed by PTT Digital who is the operator of GPSC major IT infrastructure. The process enables GPSC Group's employees can follow on suspicious activities through hotline or service desk.

In addition to escalation process from PTT digital, GPSC has the work instruction of both Operation Technology (OT) and Information Technology (IT) in place for all employees in the organization. The instructions encompass role, responsibility, and workflow between GPSC and PTT Digital team.







Escalation process for employees to report incidents, vulnerabilities or suspicious activities (2/3)

Specifically, regarding the employee escalation process, GPSC has implemented an internal Incident Management Procedure applicable organization-wide. This procedure is designed to establish a documented structure that defines the rules and standards for managing incidents effectively. It clarifies the roles and responsibilities of employees involved in incident response, promoting transparency and accountability throughout the process. The procedure outlines the methods and best practices to ensure incidents are addressed efficiently and in line with organizational policies. It also incorporates robust internal controls and approval mechanisms throughout the incident management cycle.

Incident management procedure as part of escalation process for employees

Global Power Synergy Public Company Limited	ระเบียบปฏิบัติ Procedure

ข้อมูลเอกสารฉบับล่าสุด

หมายเลขเอกสาร	PDV-P-0020	สายงาน	PSE	ฝ่าย/ส่วน	PDV
ชื่อเอกสาร	ขั้นตอนการบริหารจัดการเหตุการณ์ระบบสารสนเทศ (Incident management procedure)			สถานะ	
การแก้ไข	02	วันที่ประกาศใช้	15 ต.ค. 2567	จำนวนหน้า	16

Escalation process for employees to report incidents, vulnerabilities or suspicious activities (3/3)

Additionally, the escalation process use the priority level table to identifies the relative importance of an Incident. Incident priority is based on the combined Impact and Urgency assignments, and is used to identify the required action times. Leading to action to be activated that complies with the stepwise instruction to guide employees in executing the process correctly. Overall, this procedure ensures that incident management efforts align with business objectives and serve the best interests of the organization.

Example of priority level table

Incident Priority	4 - Urgent	3- High	2 - Medium	1 - Low

Incident Priority		Impact		
		Low (1)	Medium (2)	High (3)
Urgency	High (3)	Medium	High	Urgent
	Medium (2)	Low	Medium	High
	Low (1)	Low	Low	High

Example of Escalation process for employees to report incidents, vulnerabilities or suspicious activities

6.3 [P1] Incident Management Process

Procedure Description. In this section, the above process workflow is detailed in a more explanatory procedure description table format.

Reporter	Inform/Notify Event/System Alarm/Complaint	• Inform or notify events, system alarms, or complaints to IT Service Desk through various means, i.e., phone, email, Microsoft Teams, or Service Desk Platform. Some events or system alarms are early detected by Digital Platform Analyst themselves.

Information security awareness training

Information security awareness training (1/3)

GPSC has organized training courses on information security and cybersecurity awareness, including compliance with the company's Information and Communication Technology Policy Standard Practice, covering areas such as computer and software usage, internet access, email communication, and computer virus protection. These trainings are provided to employees at all levels, including new hires, through online platforms such as e-Learning and orientation sessions. The objective is to raise awareness of cyber threats and ensure understanding of the policies and regulations governing the use of information technology systems, which all employees must strictly follow as part of their performance evaluation. In addition to the existing curriculum, the training has been enhanced with new modules covering emerging cybersecurity topics such as ransomware attacks, the rise of cybersecurity AI, potential cybersecurity incidents projected for 2030, AI-based predictive social engineering, zero trust architecture, the role and function of Computer Emergency Response Teams (CERT), and cybersecurity incident preparedness. These additions aim to equip employees with up-to-date knowledge and readiness to respond to evolving cyber threats.

Information security awareness training (2/3)

AI Data Security Awareness

Security Patch Management Communication

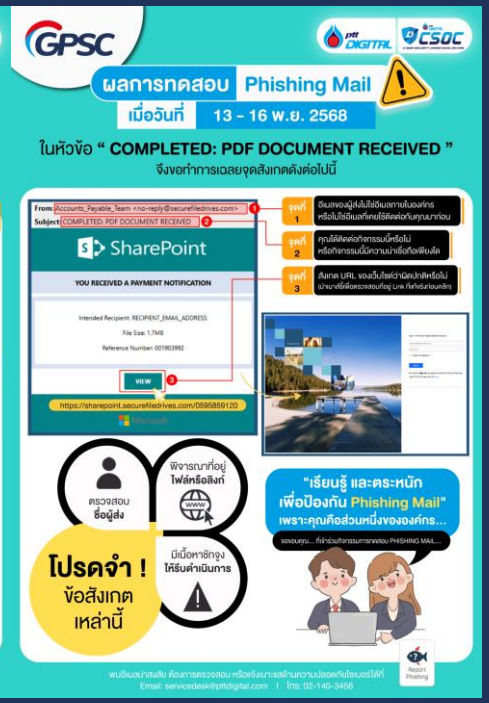
Industry Technology Awareness

Data Classification Awareness

Cybersecurity Trend Awareness

Information security awareness training (3/3)

Phishing Simulation Debrief



Phishing Prevention Guideline

Thank You