PERFORMANCE AUDIT

on Cyber Security and Resilience to Support National Security Stability

Novy G.A. Pelenkahu

Director General of Audit I, BPK RI

Jakarta, 2 September 2021

ISO 27032: Cybersecurity or the Cyberspace security, defined as the preservation of confidentiality, integrity and availability of information in the Cyberspace.

IT Governance UK defines Cyber Resilience as a measure of the ability to prepare, including the ability to respond to and recover from cyber attacks.

CISCO defines Cyber Security as the process of protecting systems, data, networks and programs from digital threats or attacks.

IT Governance Indonesia defines Cyber Security as an activity to secure telematics resources in order to prevent cyber crimes from occurring.

Kaspersky defines Cyber Security as the practice of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.

Cyber Resilience: *the ability to detect, manage dan recover from cyber security incident*.

DEFINITION OF CYBER SECURITY AND CYBER RESILIENCE

Cyber dynamic conditions covering all aspects of national life that are integrated, safe, and resilient and able to develop Indonesia's cyber strength in dealing with all cyber threats to Indonesian cyber interests and resources controlled by the Republic of Indonesia.

Cyber Security and Resilience Law, 2019

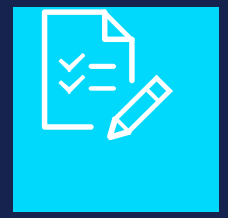
BACKGROUND OF CYBER SECURITY & RESILIENCE PERFORMANCE AUDIT (1) – WHY?

1. RECENT CYBER ATTACKS IN INDONESIA

Audit Problems in Public

- Tokopedia's e-commerce user data leak case in May 2020 totaled 91 million user data. The data is reportedly sold on the dark web, for $5,000
- Bukalapak's e-commerce user data leak case in 2015. As many as 13 million accounts were stolen and sold on dark web
- Data leak case of 279 million users of BPJS (National Health Insurance) in May 2021. The data contains full name, date of birth, national identification number (NIK), Tax identification number (NPWP), email address and cell phone number.
- The hacking of national agencies websites

2. LEGAL & ORGANIZATIONAL ASPECTS



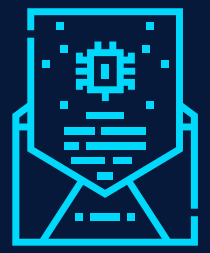
- Laws and Regulations related to cyber security are still incomplete
- Risk of overlapping roles of Ministries/ Agencies in cybersecurity
- Lack of coordination between Ministries/ Agencies in national cyber security efforts
- The risk of procuring cyber security hardware and software which may be inefficient, uneconomical, and ineffective

BACKGROUND OF CYBER SECURITY & RESILIENCE PERFORMANCE AUDIT (2)

3. *Assessing the national agenda as stipulated in the National Medium-Term Development Plan (RPJMN) 2020-2024, namely the agenda of strengthening the stability of politics, law, security, and defense*

4. *Priority Program No. 5 on the RPJMN 2020-2024 "Maintaining National Security Stability" namely "Strengthening Cyber Resilience & Security"*

5. *Implementation of SDGs Goal 16: "Peace, Justice, and Strong Institution"*



THE AUDIT OBJECTIVES

#1

Has the central government implemented cyber security and resilience effectively on the national level ?

#2

Have the Ministries/Agencies implemented cyber security and resilience effectively? (at 5 Ministries/Agencies sampled)

THE AUDIT SCOPE

Assess the effectiveness in planning, implementation and monitoring related to:

1. Regulations and policies (Legal);
2. Standardization/Procedures/Protocols (Technical);
3. Institutional/Organizational;
4. Resource Development (Capacity Development);
5. Cooperation (Cooperation).

THE AUDITEES – Audit Scope

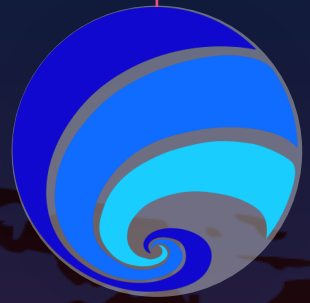
National Cyber and Crypto Agency (BSSN)

Cybersecurity Center Ministry of Defense

National Intelligence Agency (BIN)

Directorate of Cybercrime Indonesian National Police

Ministry of Communication and Information Technology



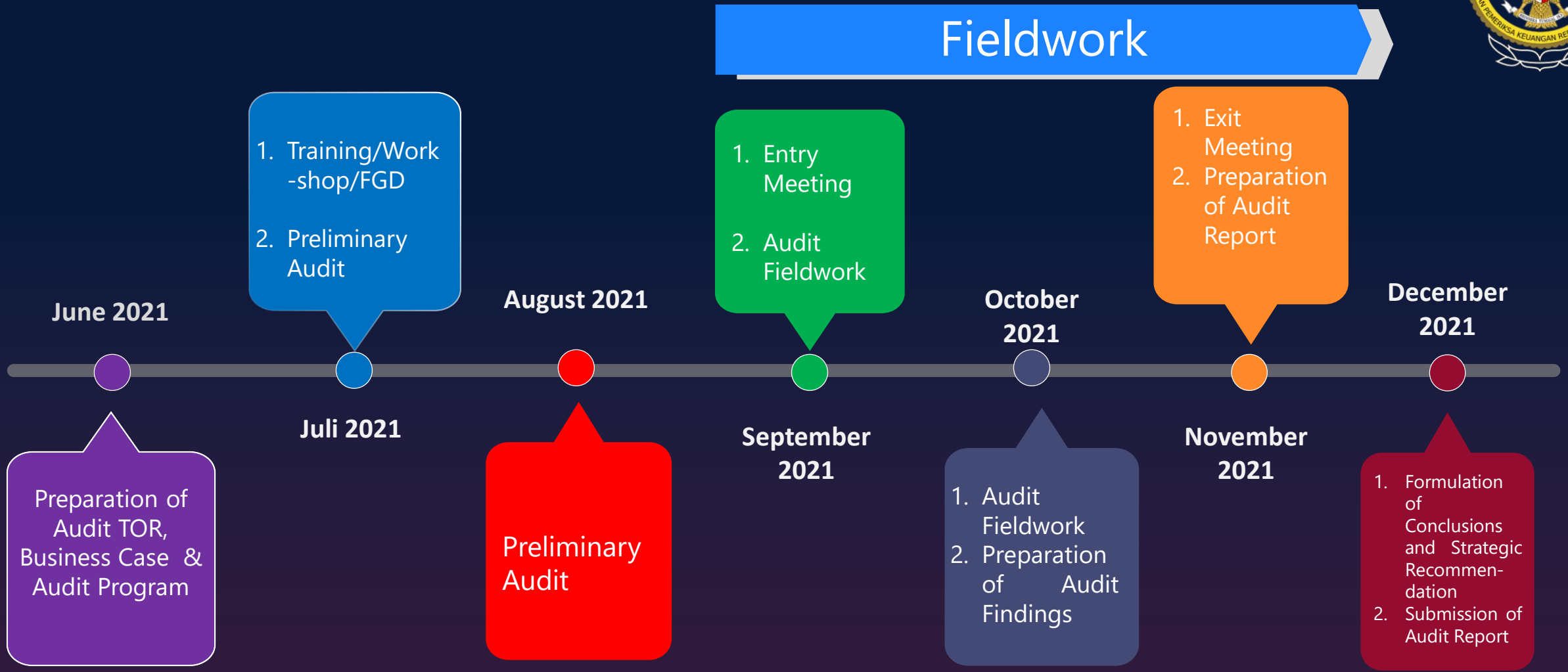
THE AUDIT METHODOLOGY

We are using **a problem-oriented approach**, which examines, verifies and analyses the causes of particular problems or deviations from criteria.

What we are doing in data collection.

1. Collecting and reviewing relevant laws and regulations (including international best practices) related to cyber security function of the relevant Ministries/Agencies
2. Collecting and analyzing data or information through interviews, observations, and questionnaires in order to understand the systems, mechanisms, and procedures for cyber security tasks and functions in related Ministries/Agencies
3. Collecting relevant data and information through various media to obtain current issues regarding cyber security and resilience
4. Identification of performance indicators, targets, risks and weaknesses in related Ministries/Agencies cyber security functions
5. Discussions with management regarding systems, mechanisms, and procedures as well as efforts to achieve targets in the duties and functions of cyber security in related Ministries/Agencies
6. Focus group discussion with some related experts
7. Benchmarking activities, to compare cyber security and resilience practices in other countries

THE AUDIT TIMELINE



AUDIT RESOURCES

Audit Teams	Personnel/Auditor Involved
National Cyber and Crypto Agency (BSSN)	11
Ministry of Defense	11
National Intelligence Agency (BIN)	6
Indonesian National Police	9
Ministry of Communication and Information Technology	6
Total	43

Technical Knowledge Necessary within The Audit Team

The team should have knowledge of:

- cyber security principles
- government requirements and guidance
- network security
- security assessment and authorisation
- risk management
- cyber defence and vulnerability tools

AREAS OF IMPROVEMENT

We found area of improvement related some aspects including legal, technical, organizational, capacity development and cooperation.

We also give some recommendations related those aspects. Some of our important recommendations are:

(1) Each ministries/agencies should be responsible to maintain its cyber security aspects following proper guidance set by the National Cyber and Crypto Agency

(2) The Government prepares guidelines related to HR competencies and standards for facilities and infrastructure needed to support their activities in strengthening cyber security and cyber resilience

(3) The Government should enhance cooperation with the private sector, national critical sectors, and between ministries/agencies in the field of cyber security which includes information sharing, access, and joint capacity building.


TRI DHARMA
ARTHASANTOSHA
BADAN PEMERIKSA KEUANGAN REPUBLIK INDONESIA

THANK YOU