TURN
KNOWLEDGE
INTO PERFORMANCE
CATALYZING GREATER IMPACT FOR GREATEST VALUE

ultimatics
turn knowledge into performance

ADVANCING CYBER RESILIENCE AND MATURITY

LEVERAGING ISO 27001:2022 AND NIST CSF 2.0 FOR ENHANCED SECURITY POSTURE

TEDDY AZTA

Session Agenda

Outline of Key Discussion Points

1 What to Expect

An overview of the session, including the background, frameworks discussed, and case studies presented.

2 Background

Discussion on the foundational concepts related to advancing cyber resilience.

3 Frameworks

Introduction to key frameworks such as ISO 27001:2022 and NIST CSF 2.0 that guide the maturity journey.

4 Case Study

Examination of a real-world example demonstrating successful implementation and outcomes.

5 Recommendations

Actionable insights and strategies for enhancing cyber resilience based on findings.

Cybersecurity Landscape in Indonesia

Current Threats and National Cybersecurity Readiness

1

Key Cybersecurity Threats

Ransomware, phishing, and insider risks are the most prevalent threats facing organizations in Indonesia.

2

Incident Statistics Overview

National data indicates an upward trend in cybersecurity incidents impacting businesses and critical infrastructure.

3

National Cybersecurity Readiness

Institutions like BSSN and OJK lead initiatives to enhance cybersecurity resilience and compliance nationally.

Common Challenges in Indonesian Organizations

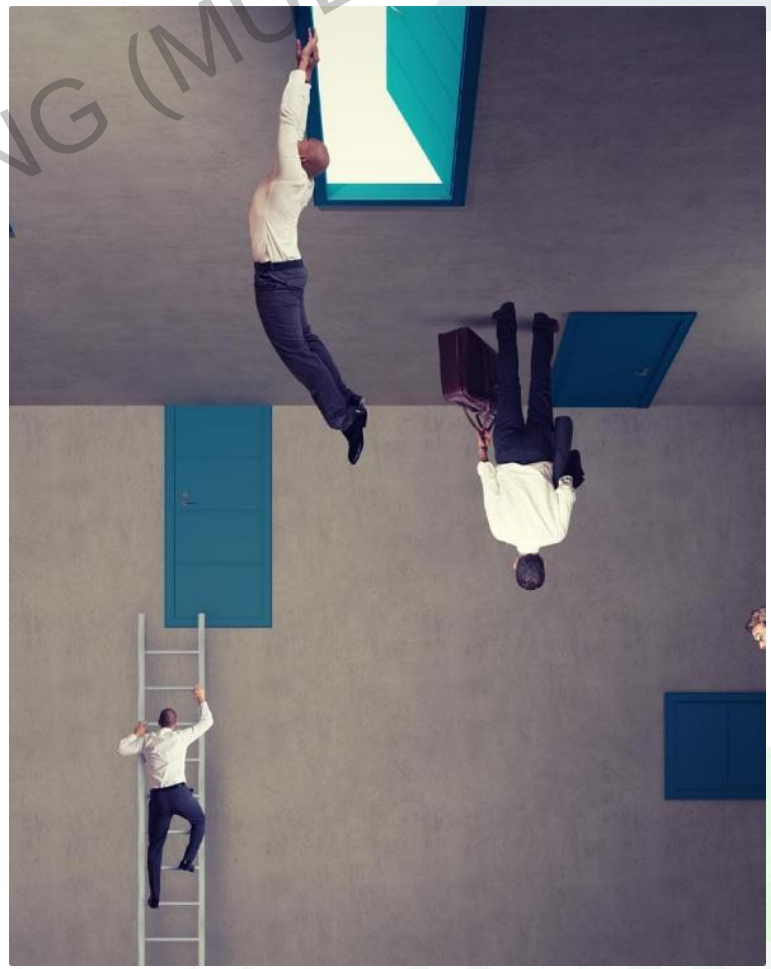
Understanding Key Issues Faced

Challenges

- **Policy fragmentation**: Diverse regulations and guidelines lead to confusion and inefficiencies.
- **Limited cybersecurity talent**: A shortage of skilled professionals hinders effective security measures.
- **Lack of integrated governance**: Absence of cohesive governance frameworks can cause fragmented decision-making.
- **Resource constraints**: Financial and human resources are often limited, impacting the ability to implement solutions.

Implications

- **Operational inefficiency**: Confusion can lead to delays and ineffective operations.
- **Increased vulnerabilities**: A lack of talent increases susceptibility to cyber threats.
- **Decision paralysis**: Fragmentation may cause slow responses to emerging issues.
- **Inadequate solutions**: Limited resources can lead to compromised security and governance frameworks.



Why Cyber Resilience Matters

Understanding the Critical Difference

1

Operational Disruption

Cyber incidents can halt business processes, leading to significant loss in productivity and service delivery.

2

Financial Consequences

The financial damage from cyberattacks can be immense, including recovery costs and lost revenue.

3

Regulatory Impact

Non-compliance due to lapses in cyber resilience can lead to hefty fines and legal issues.

4

Reputation Damage

Falling victim to cyber threats can tarnish an organization's reputation, affecting customer trust.

Frameworks at a Glance

Understanding ISO 27001:2022 and NIST CSF 2.0

PURPOSE OF ISO 27001

Establishes information security management systems to protect organizations' data.

1

NIST CSF OVERVIEW

Framework to improve the security management of critical infrastructure through guidance and best practices.

2

COMMON GOALS

Both frameworks aim to boost organizations' resilience against cyber threats and manage risks effectively.

3

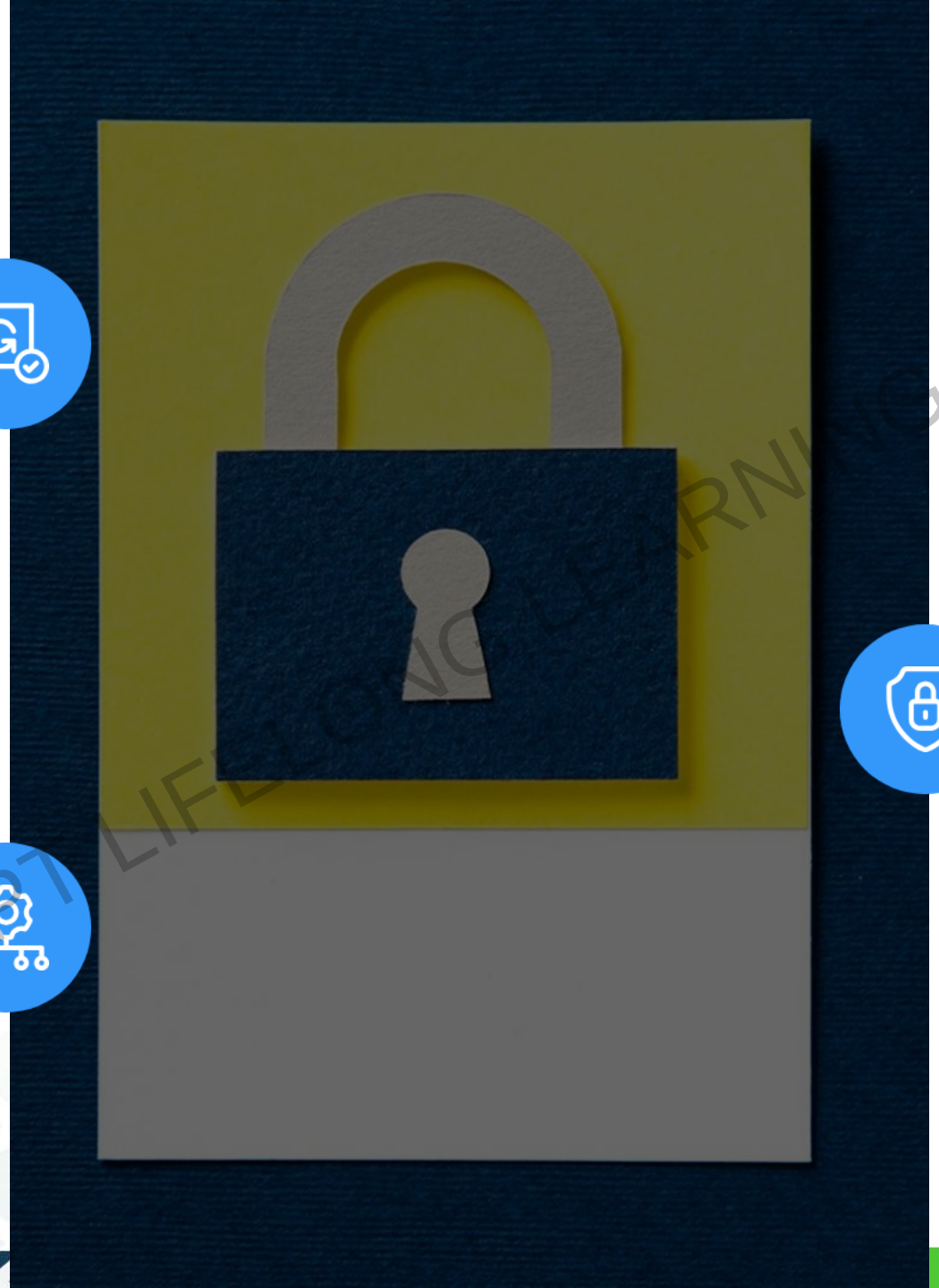
COMPLIANCE REQUIREMENTS

ISO 27001 includes certification, while NIST CSF focuses on voluntary adoption of its principles.

4

Major Updates from 2013

ISO 27001:2022 introduces significant changes that enhance information security management practices.



Modernized Security Controls

Updates the existing controls to better fit with current cybersecurity threats and practices.

Focus on Organizational Context

Emphasizes understanding the organizational context, leading to tailored security controls.

Highlights of NIST CSF 2.0

Key updates and enhancements from NIST CSF 1.1.

1 Evolution from Version 1.1

The NIST Cybersecurity Framework has undergone significant updates, evolving from its previous iteration to better address current cybersecurity challenges.

2 Introduction of 'Govern'

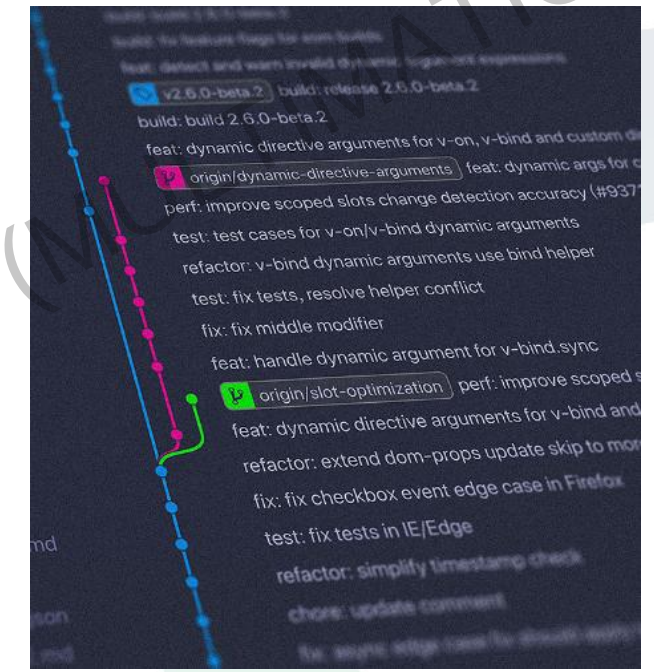
The new 'Govern' function focuses on governance aspects of cybersecurity, emphasizing the importance of leadership and organizational structures.

3 Outcome-Based Approach

The outcome-based approach in CSF 2.0 allows organizations to prioritize cybersecurity outcomes, enhancing strategic planning and resource allocation.

Comparison: ISO 27001 vs NIST CSF 2.0

Key Aspects and Complementarity



ISO 27001

1. **Framework**: Standards-based approach.
2. **Focus**: Certification and risk management.
3. **Applicability**: Broad, across industries.
4. **Complementarity**: Integrates with NIST CSF.

NIST CSF 2.0

1. **Framework**: Flexible, best practices.
2. **Focus**: Cybersecurity outcomes and improvements.
3. **Applicability**: Primarily for U.S. critical infrastructure.
4. **Complementarity**: Enhances ISO 27001 implementation.

Hybrid Approach: Mapping and Integration

Combining ISO and NIST CSF to Enhance Cyber Resilience in Indonesia

Getting Started with Cyber Maturity

Assessing Current State Against Frameworks

Current State Assessment

Evaluate the current cybersecurity posture against established frameworks to identify gaps and areas for improvement.

1

2

Framework Comparison

Utilize both ISO 27001:2022 and NIST CSF 2.0 as benchmarks for thorough evaluation and enhanced strategy formulation.

Governance and Leadership Commitment

Highlighting the Role of Executive Management

Executive Management Role

1. Sets the strategic **direction**.
2. Ensures **alignment** with business goals.
3. Drives **organizational culture** support.
4. Fosters a **risk-aware** environment.

Three Lines of Defense

1. First line: **Operational Management**.
2. Second line: **Risk Management** functions.
3. Third line: **Independent Assurance**.
4. Supports **compliance** and **effectiveness**.

Phased Implementation

Strategic prioritization by risk and impact

Implement priority initiatives balancing risk reduction and resource allocation for sustained progress.

Mid-term Goals

Phase 2

Phase 1

Quick Wins

Focus on rapid, high-impact actions to deliver immediate benefits and build momentum.

Phase 3

Long-term Vision

Establish comprehensive, future-focused measures for enduring cyber resilience and maturity.

Local Case Study

Detailed Snapshot of Indonesian Success

Implementation Depth in Indonesia

Exploring the detailed and effective deployment of the solution within Indonesian context highlighting strategic steps.

Achieved Tangible Benefits

Clear measurable outcomes and benefits realized post-implementation showcasing return on investment and operational improvements.

Human Factor: Capacity Building & Culture

Enhancing Security Through Robust Awareness Programs

Awareness Programs
Implementing tailored awareness programs is essential to educate employees about security risks and best practices.

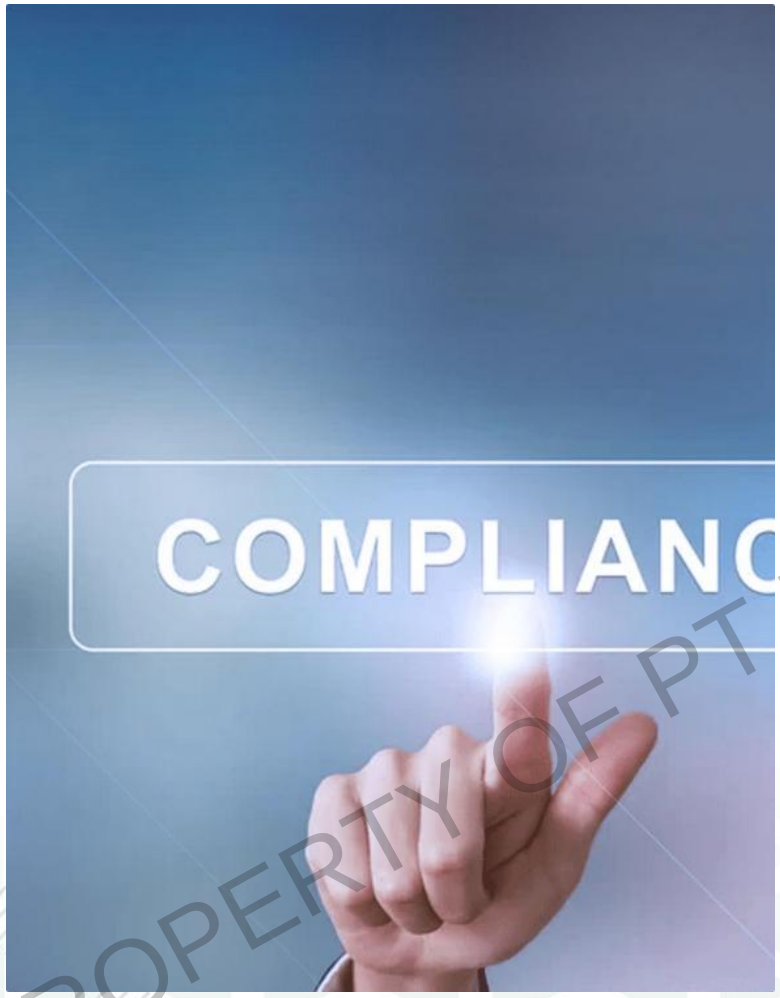
Training Initiatives
Regular training ensures that employees are updated on the latest threats and how to counter them effectively.

Accountability Measures
Establishing accountability among employees fosters a culture of responsibility regarding security protocols and practices.

Fostering Security Culture
Cultivating a strong security culture can significantly reduce risks by encouraging proactive behaviors among staff.

Regulatory Alignment & Localization Needs

Ensuring compliance with essential guidelines to enhance cyber resilience.



Synchronizing with POJK

Aligning organizational practices with the latest requirements set by POJK for optimal governance.

Following PP PSTE Guidelines

Implementing the directives of PP PSTE to ensure secure and resilient operations.

Adhering to BSSN Standards

Complying with BSSN regulations to fortify national cybersecurity infrastructure.

Integration with SNI ISO

Incorporating SNI ISO standards as a benchmark for quality and security in processes.

Business Benefits of Cyber Maturity

Understanding the advantages of enhancing cyber resilience and maturity.

Compliance with Standards

Adhering to industry standards strengthens legal compliance, reducing risk of penalties.

Enhanced Partner Trust

Demonstrating high levels of cyber maturity increases trust among partners and clients.

Operational Efficiency

Improved cyber practices streamline operations, leading to better resource utilization.

Human Factor: Capacity Building & Culture

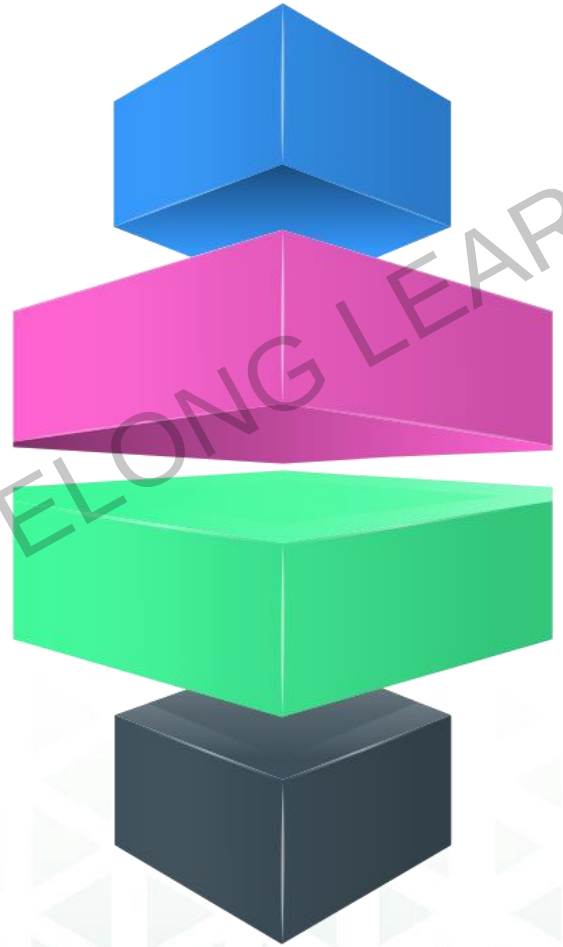
Enhancing Security Through Robust Awareness Programs

Advisory Services

Consultants provide expert advice to guide organizations in strategic decision-making and transformations.

Roadmap Development

Creating actionable plans that define how organizations can achieve their transformation goals effectively.



Assessment Processes

Conducting thorough assessments to identify gaps and areas of improvement for better performance.

Audit Preparation

Helping businesses prepare for audits by ensuring compliance with necessary standards and frameworks.