Template for CISO's Presentation on the DORA Regulations

To CEOs & Board of Directors

Balbix®

⚠ Delete this slide after use

General Directions

This presentation template includes key slides on the Digital Operational Resilience Act (DORA) that you can present to your CEO or the board of directors

Directions

- The core presentation is Slides 3-10. Other slides contain instructions and additional materials
- Customize these slides based on the unique context of your organization and industry
- Use the slides in the appendix section as needed to augment the presentation

⚠ Delete this slide after use

DORA Cybersecurity Rule Overview

April 2024

Summary

1. What is DORA?
2. DORA Implementation Timeline
3. DORA Requirements
4. DORA Key Concepts
5. Most Important Concept – Materiality
6. Next Steps Toward DORA Compliance

What is DORA?

The DORA Act (Digital Operational Resilience Act), is part of the European Union's efforts to enhance the digital operational resilience of its financial sector. The primary aim of DORA is to ensure that all entities in the financial system have the necessary safeguards in place to mitigate cyber attacks and other risks related to their digital operations. The act goes into effect **Jan 17, 2025.**

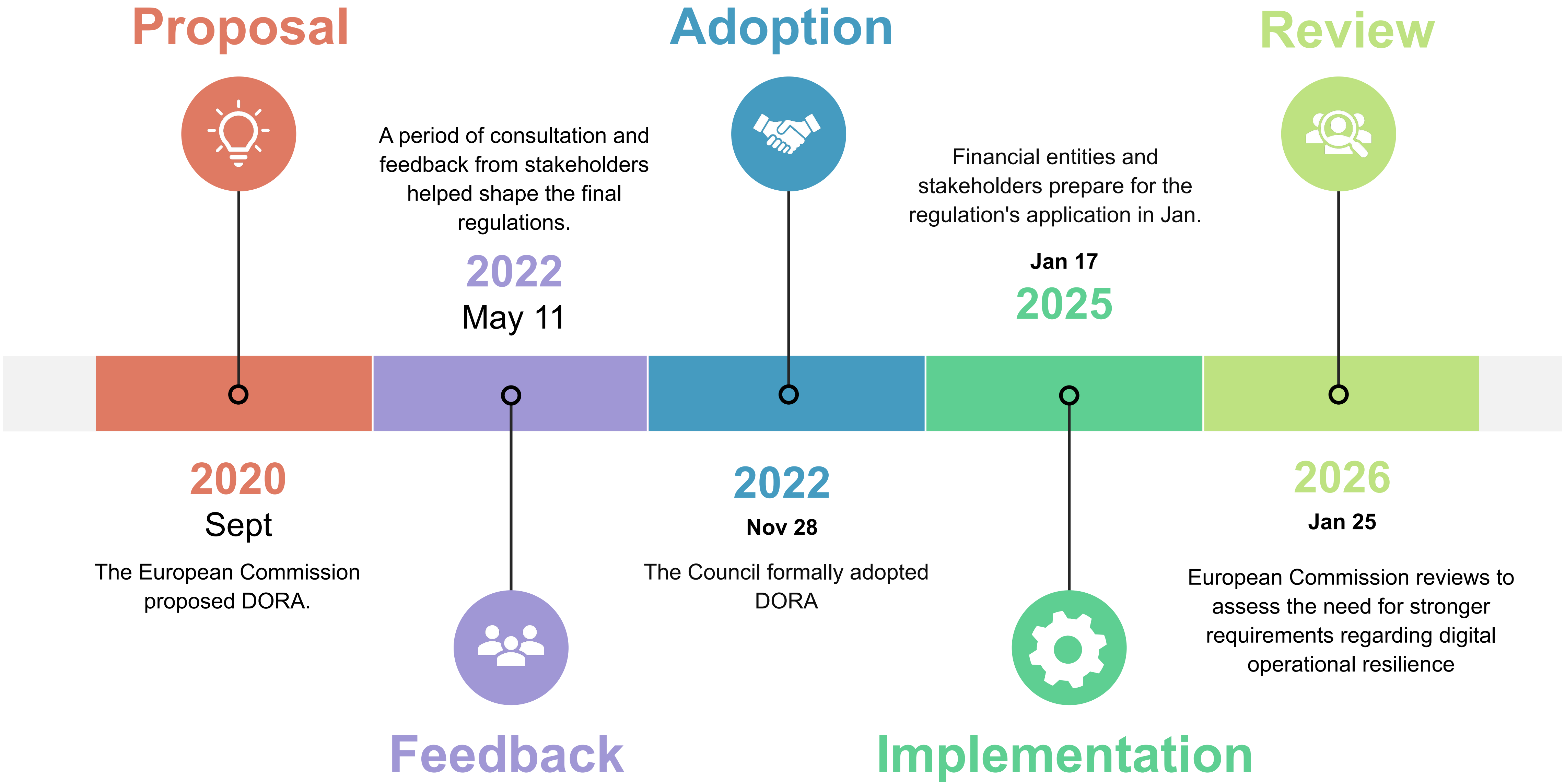
For the Financial Entity

DORA aims to strengthen cybersecurity and operational resilience of financial entities and their service providers.

For the EU

DORA aims to ensure the stability and integrity of the financial markets.

DORA Implementation Timeline



Proposal

2020

Sept

The European Commission proposed DORA.

Feedback

2022

May 11

A period of consultation and feedback from stakeholders helped shape the final regulations.

Adoption

2022

Nov 28

The Council formally adopted DORA

Implementation

Jan 17

2025

Financial entities and stakeholders prepare for the regulation's application in Jan.

Review

2026

Jan 25

European Commission reviews to assess the need for stronger requirements regarding digital operational resilience

DORA Requirements

ICT Risk Management	Incident Reporting	Digital Operational Resilience Testing	ICT Third-Party Risk Monitoring	Information Sharing & Intelligence
Financial entities must establish and maintain a comprehensive risk management frameworks capable of identifying, assessing, mitigating, & managing ICT risks.	Financial entities must promptly report significant cybersecurity incidents to relevant authorities, typically within 72 hours.	Financial entities must regularly test their ICT systems & processes to ensure they can withstand & recover from operational disruptions.	Financial institutions must oversee & manage risks associated with third-party ICT service providers.	Financial entities are encouraged to share information about cyber threats, vulnerabilities, incidents, & best practices.
Key Elements: • Risk assessment • Define policies & procedures • Protection & prevention • Incident response & recovery plans	**Key Elements:** • Define reporting thresholds • Timely notification • Detailed reporting • Mitigation plan	**Key Elements:** • Penetration testing • Scenario-based testing • Testing frequency and rigor	**Key Elements:** • Due diligence • Contractual Agreements • Ongoing monitoring	**Key Elements:** • Establishing information-sharing arrangements with peers • Protecting shared information • Leveraging intelligence to improve cyber posture

DORA Key Concepts

01 **MATERIALITY**

This refers to the significance of an event, fact, or item. Materiality matters because it can influence decisions, affect interpretations, or change outcomes.

02 **RISK ASSESSMENT/MANAGEMENT**

This involves the identification, evaluation, and prioritization of risks, and the application of resources to minimize, control, and mitigate their impact. A business might assess the risk of a data breach and manage it by enhancing their cybersecurity measures.

03 **INCIDENT REPORTING**

This is the process of documenting all details of an event that could possibly result in personal injury or damage to property. For instance, if a worker is injured on a construction site, an incident report would be necessary to document what happened and why.

04 **GOVERNANCE**

Governance refers to the structures and processes in place for managing an organization and guiding its path towards achieving its goals. An example of this could be a corporation's board of directors who set the strategic direction and oversee the management of the company.

05 **OPERATIONAL RESILIENCE**

This is an organization’s ability to withstand, adapt to, and recover from disruptions while continuing to serve its customers or perform its critical operations. A bank, for example, may demonstrate operational resilience by ensuring it can still operate during a power cut or cyber attack.

The Most Important Concept—Materiality

How does DORA define it

- The significance of an incident's impact on the ICT systems and processes of a financial entity.
- Takes into account factors such as the potential harm to consumers, financial markets, and the stability of the financial system.

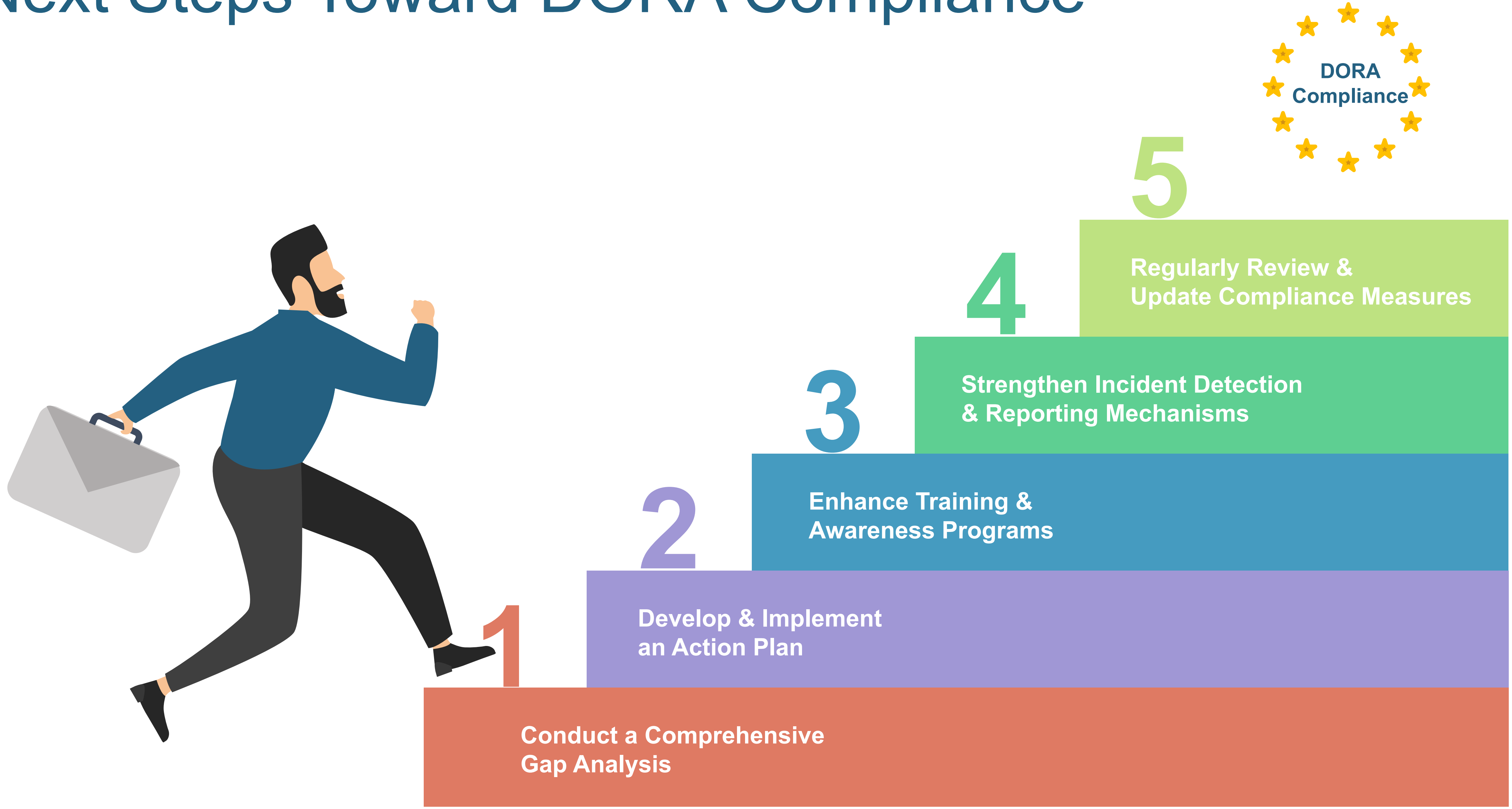
Who should be involved

- Multiple stakeholders across leadership, risk management, compliance and cybersecurity departments.
- Chief Risk Officers (CROs), Chief Information Security Officers (CISOs)
- Build a playbook for identifying material incidents, disclose criteria.

Addressing grey areas

- When in doubt, disclose.
- The 72-hour reporting window for material cyber incidents begins upon incident detection.

Next Steps Toward DORA Compliance



DORA Compliance

5 Regularly Review & Update Compliance Measures

4 Strengthen Incident Detection & Reporting Mechanisms

3 Enhance Training & Awareness Programs

2 Develop & Implement an Action Plan

1 Conduct a Comprehensive Gap Analysis

If you found these slides helpful

Balbix can help you determine materiality and comply with DORA cybersecurity requirements.

Balbix will help you provide visibility into your all your assets and automate critical elements of your cybersecurity program and quantify changes in risk as you improve your cybersecurity posture. The next few slides has some additional examples.

⚠ Delete this slide after use

How Balbix can help

Balbix®

Materiality determination

Balbix can help you determine **whether an incident, application, asset, threat or vulnerability is material,** by analyzing all data from IT, security, and business tools and identifying if they pose material risk to the organization

Cyber risk management

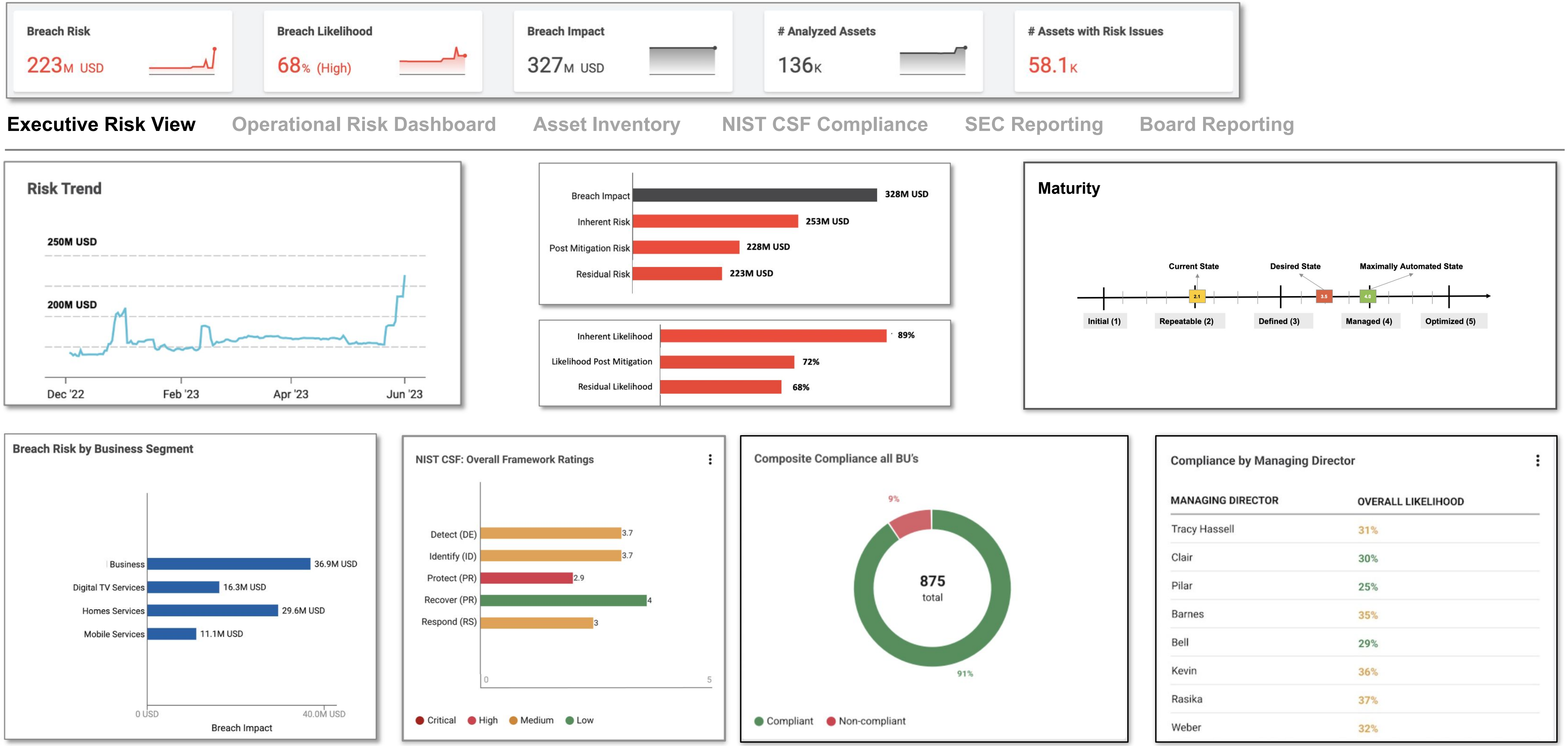
Balbix can help you to quantify and **manage material cyber risks** down to acceptable levels with a data-driven model that be traced to specific assets

Governance and compliance

Balbix enables you to unify cyber governance, operational cybersecurity, and compliance to enable better management of **material cyber risks in a single platform**

⚠ Delete this slide after use

Sample Executive Risk View



Breach Risk 223M USD

Breach Likelihood 68% (High)

Breach Impact 327M USD

Analyzed Assets 136K

Assets with Risk Issues 58.1K

Executive Risk View | Operational Risk Dashboard | Asset Inventory | NIST CSF Compliance | SEC Reporting | Board Reporting

Compliance by Managing Director

MANAGING DIRECTOR	OVERALL LIKELIHOOD
Tracy Hassell	31%
Clair	30%
Pilar	25%
Barnes	35%
Bell	29%
Kevin	36%
Rasika	37%
Weber	32%

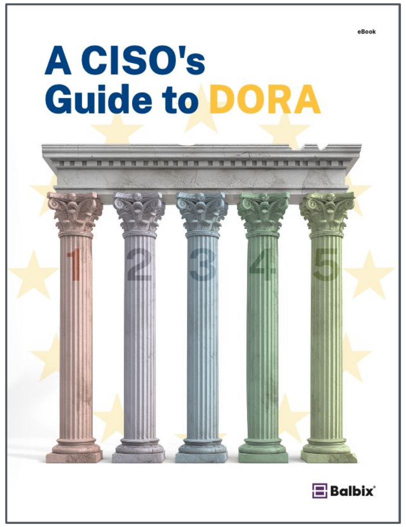
⚠ Delete this slide after use

Resources

Balbix®

eBook

A CISOs Guide to the DORA



eBook

A CISO's Guide to DORA

Balbix

Includes an explanation of DORA requirements and how Balbix can help address them.

Download Now

Webinar

Master the EUs latest Cybersecurity Regulation

Webinar

Balbix

DORA: Practical Insights on How to Achieve Cyber "Resilience"

Paul Kelly
DORA Expert, Security Strategy Advisor

Sid Wahi
Sr. Director, Product Management Balbix

What you will learn

- What's DORA's impact on the organization?
- How do you get started?
- What changes might your organization need to implement DORA?
- How can AI and Automation help you fast-track DORA compliance?

Watch the Video

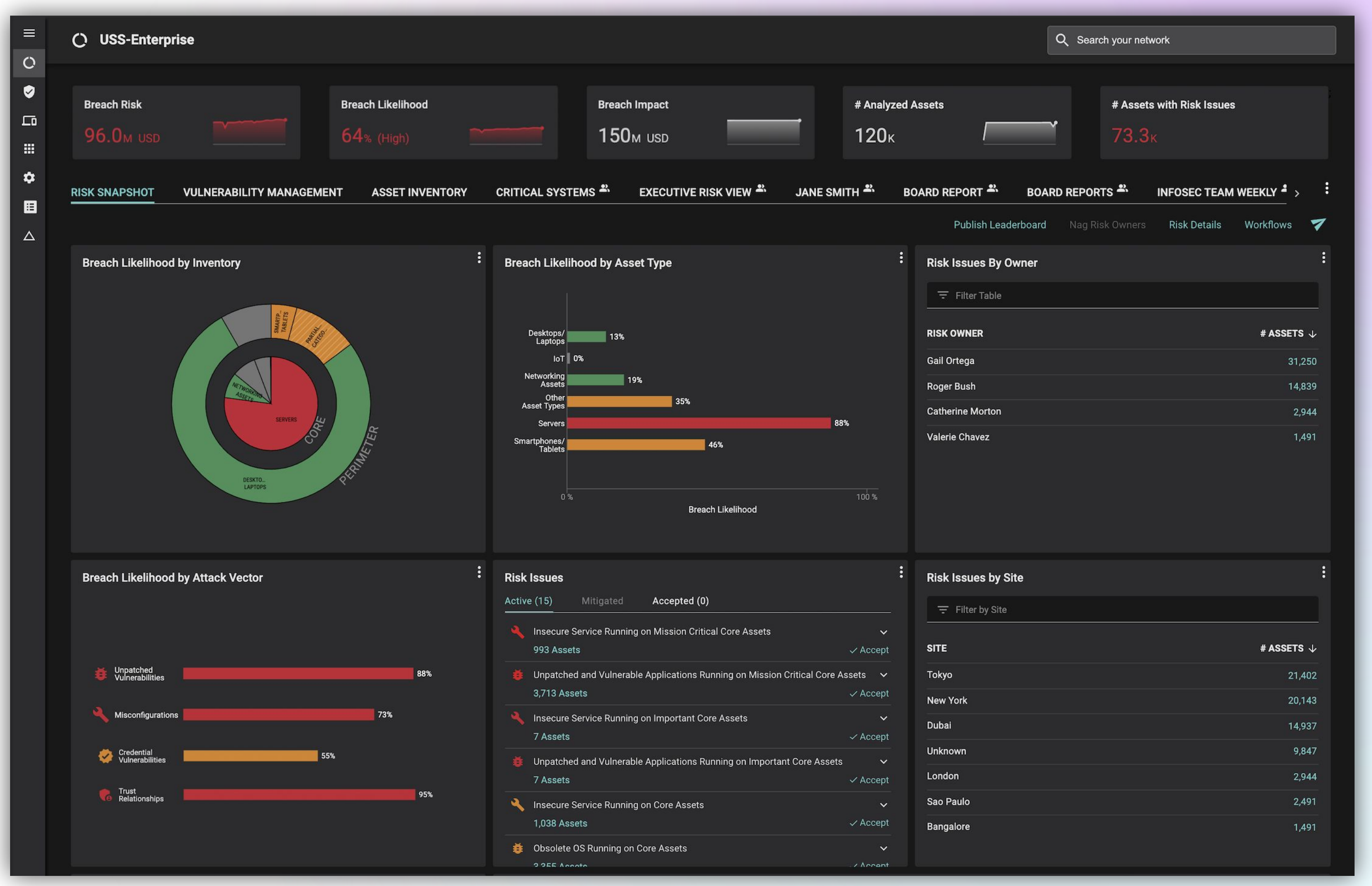
⚠ Delete this slide after use

In 30 minutes, we will show how Balbix can provide visibility into all your assets including your material assets.

Additionally, you will be able to quantify your cyber risk in $-terms, traceable to operational metrics and asset attributes driving this risk.

Request a Demo

Balbix®



Risk Issues By Owner

RISK OWNER	# ASSETS ↓
Gail Ortega	31,250
Roger Bush	14,839
Catherine Morton	2,944
Valerie Chavez	1,491

Risk Issues

Active (15) Mitigated Accepted (0)

Insecure Service Running on Mission Critical Core Assets
993 Assets ✓ Accept

Unpatched and Vulnerable Applications Running on Mission Critical Core Assets
3,713 Assets ✓ Accept

Insecure Service Running on Important Core Assets
7 Assets ✓ Accept

Unpatched and Vulnerable Applications Running on Important Core Assets
7 Assets ✓ Accept

Insecure Service Running on Core Assets
1,038 Assets ✓ Accept

Obsolete OS Running on Core Assets
3,355 Assets ✓ Accept

Risk Issues by Site

SITE	# ASSETS ↓
Tokyo	21,402
New York	20,143
Dubai	14,937
Unknown	9,847
London	2,944
Sao Paulo	2,491
Bangalore	1,491

A single, comprehensive view of cybersecurity posture

⚠ Delete this slide after use