20TH ANNIVERSARY EDITION

WSO2CON ASIA

PLATFORMLESS MODERNIZATION

Compliance Without Slowing Down Innovation

Nevi Amunugama
VP & CISO
WSO2

Innovation and Software Development

Credit: Thinkstock

Industry Recognitions
https://wso2.com

Forrester Wave 2023

KuppingerCole 2024

Gartner Peer Insights Customers Choice 2023

Innovation is the bedrock of software development

- Innovation is at our core & fundamental to everything we do at WSO2.
- We are not just a software development leader. We deliver securely with open source technology and at scale.
- This steppingstone called “innovation” will remain throughout the lifecycle of our products & services.
- Innovation drives growth, attracts customers & investors, and established us as a leader in the market .

WSO2 Security & Compliance:
https://wso2.com/security/

It's all about the balance!

- Must change the perception and traditional ideology: "*Security & Compliance slows down innovation*"
- Encourage adoption of new technologies.
- Bring together collaboration, innovation, security & compliance to be building blocks that make & define our products and services. As a result,
  - Hold a stronger position in the market
  - Sustain effectiveness with customers over time
  - Be resilient
  - Maintain the confidence you have with customers
  - Explore markets across the globe.
- Manage this balance from a Cyber, operational, legal, finance and business perspective - No pressure!
- **Question**: *"So, what's the Risk?"*

Compliance at WSO2

Compliance at WSO2

Fundamental principles of compliance

- Security Compliances at WSO2
  - Strategic approach to applicability
  - lifecycle management
- Compliance will always be an opportunity and not a blocker for innovation and creativity
- Improves product development efficiency & optimization
- Encourage collaboration, new ideas and creativity

Compliance at WSO2

Regulatory/ Certifications /Attestations

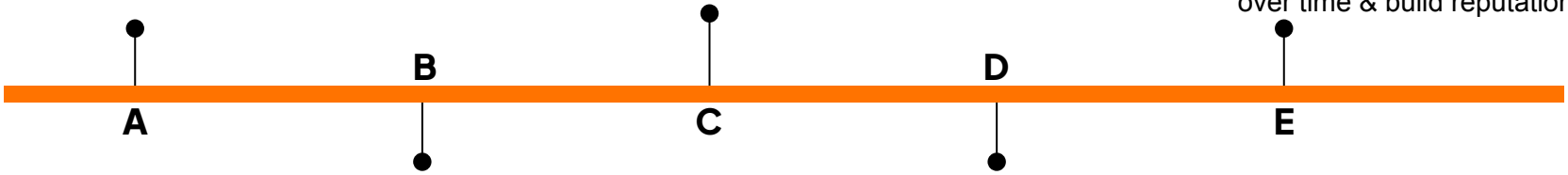
- ISO27001
- SOC 2 Type 2
- HIPAA
- PCI

Coverage Scope

- SaaS products & Open Source On-Prem Deployments
- Market our products across the world with little change
- Cross functional engineering & security support to meet compliance

Deliver compliant products at scale

- Accountability, delivery, industry best practice & reasonableness are all part of this process
- Operational effectiveness in compliance = competitive advantage
- Gain customer confidence, sustain over time & build reputation.



Regional/Customer/ Deployment specific

- GDPR
- DORA (EU)
- CCPA
- DPO
- Privacy
- ENS (EU)
- RBI (India)
- CRA (EU)
- Data Protection (Japan)
- Data Privacy (Philippines)
- Data Privacy (SL)
- AI Act (EU)
- NIS 2 (EU)

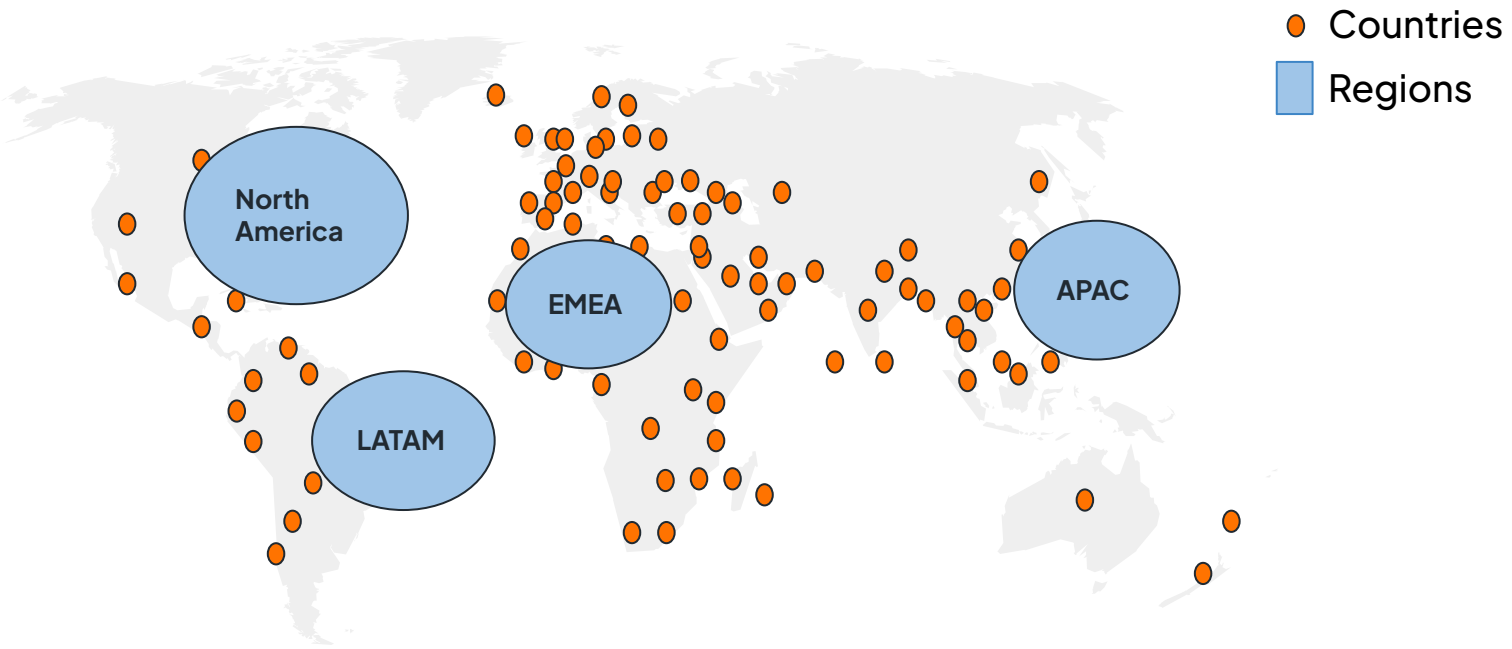
GRC Function

- Fully integrated with compliance lifecycle
- Flexible and help meet business goals
- Balance innovation, deployment speed and compliance
- Less rigid & handles agile workflows with rapid changes
- Decentralized decision making with clear indication of must have requirements vs opportunities for innovation

*Work in progress

Security

Compliance at WSO2 – Customers



** All individual countries not represented due to space limitations.*

Compliance at WSO2 – innovation and creativity

It is an opportunity, not a blocker

- The many regulatory compliance certifications & regional compliance requirements that we manage has pushed us to be more creative and innovative to deliver at scale.
- You have to think out of the box. Stop thinking about just checking the box and following the traditional path.
- Incorporate regular compliance testing throughout the development lifecycle, teams ensure that their software remains compliant with legal standards as regulations evolve.
- Automated compliance monitoring tools provide real-time insights into potential compliance risks, allowing teams to address issues proactively.
- Examples:
  - Creative ways of achieving DORA compliance for EU banking customers
  - The evolution of another common controls matrix to drive products & services. Adding a new requirement, control or capability must feel seamless.
  - Provide ability for engineers to test innovative ideas for compliance with minimal complexity and approvals, before production.
  - Absolutely encourage new technology like the use of AI. Not be afraid and handle the security/compliance concerns

Compliance at WSO2 – Optimization

Improves efficiency with product development

- Achieving compliance by design is the most secure approach by default with capabilities to scale across products
- Compliance is inherently based on best practice. Basic principles of security are covered at design/architecture, which will then reduce potential future risks.
- Leverage compliance activities and initiatives to streamline/secure operations resulting in faster deployment timelines.
- Integrate built in compliance to the development lifecycle from the start, enables teams to avoid costly mistakes and revisions later.
- Examples:

    - Internal Audit function to help teams prepare
    - Streamlining our process to achieving compliance for cloud platforms enable us to easily add, extend instances & deployments while seamlessly achieving compliance. No additional work.
    - SDLC is mostly scanning based on automated tools with less manual steps.
      https://security.docs.wso2.com/en/latest/security-processes/secure-software-development-process/
      https://security.docs.wso2.com/en/latest/security-processes/cloud-security-process/

Compliance at WSO2 – incorporates new ideas and creativity

Encourages collaboration

- All teams need to work together and in sync for compliance in order to not slow down delivery.
- The only way to stay ahead and deliver at scale and speed is to be lock step with engineering, legal, security, product teams, customers etc.
- Given our open source technology the approach to security and compliance gets to be very collaborative & community oriented in order to access new ideas and solve unique problems.
- At WSO2 teams work to leverage cross functional efficiencies. Security teams tend to be smaller and more focussed with less operational hierarchical structures.
- Examples:
  - Annual Cyber Hackathons to keep our creativity and energy alive
  - Executing RFI's, DPA's, policies, contract terms, external/internal audits, risk registers etc.

GRC
(Governance, Risk & Compliance)

GRC at WSO2

People

Technology

Process

GRC at WSO2

Governance: Flexible & Meet Business Goals

Must include a structured framework, defined scope & agreed upon process to manage organizational security risks.

Must be aligned with strategic objectives of the organization.

- Rules, policies & roles
- Oversight Mechanisms for continuous monitoring, enforcement & improvement (Audits, reviews, assessments, tooling)
- Develop roadmap & reporting
- Tracking via risk registers
- Comms and escalation strategy

Compliance: Data Driven Decision Making

Empower our best minds to embrace creativity without fear and enable innovation with our solutions.

Compliance data must be current, dependable, repeatable, interchangeable & evidentiable.

- Pull rapid feedback to validate state
- Full scope coverage with completeness check
- Leverage existing controls and level up (common controls)
- Automate execution AND evidence collection for status tracking/readiness

Risk based approach to Compliance

Compliance is never a straight forward. It depends on the situation at hand and the true impact to your organization.

- Customize a risk management methodology that addresses your core compliance principles.
- Consistent guidance on how we detect, assess, rate and defend.
- Follow control execution, assess mitigation & compensating controls to reduce residual risk.
- Determine a balanced yet effective risk thresholds for ratings.
- Trends, forecasting & business

Use Risk Management to drive Governance

"The most innovative companies are not the ones that ignore regulations, but those that design with them in mind from the start." – *Brad Smith, President, Microsoft*

“If you think compliance is expensive, try non-compliance” - *Former US Deputy AG Paul McNulty.*

“Good compliance is good business. It encourages trust, and trust is the currency of innovation.”– *Ginni Rometty, former CEO, IBM*

"Innovation in regulated industries isn't about breaking the rules—it's about rethinking what's possible within them."
– *Mary Barra, CEO, General Motors*

Thank you!