Prepare for DORA with aligned solution architecture

Nerijus Pažereckas, Head of Architecture

June 13th, 2024

baltic amadeus

DORA

- Risk Management
- Incident Reporting
- Digital Operational Resilience Testing
- Third-Party Risk Management
- Information Sharing
- Governance and Oversight
- Business Continuity
- Resilience in Critical Services

baltic amadeus

Well-Architected Framework

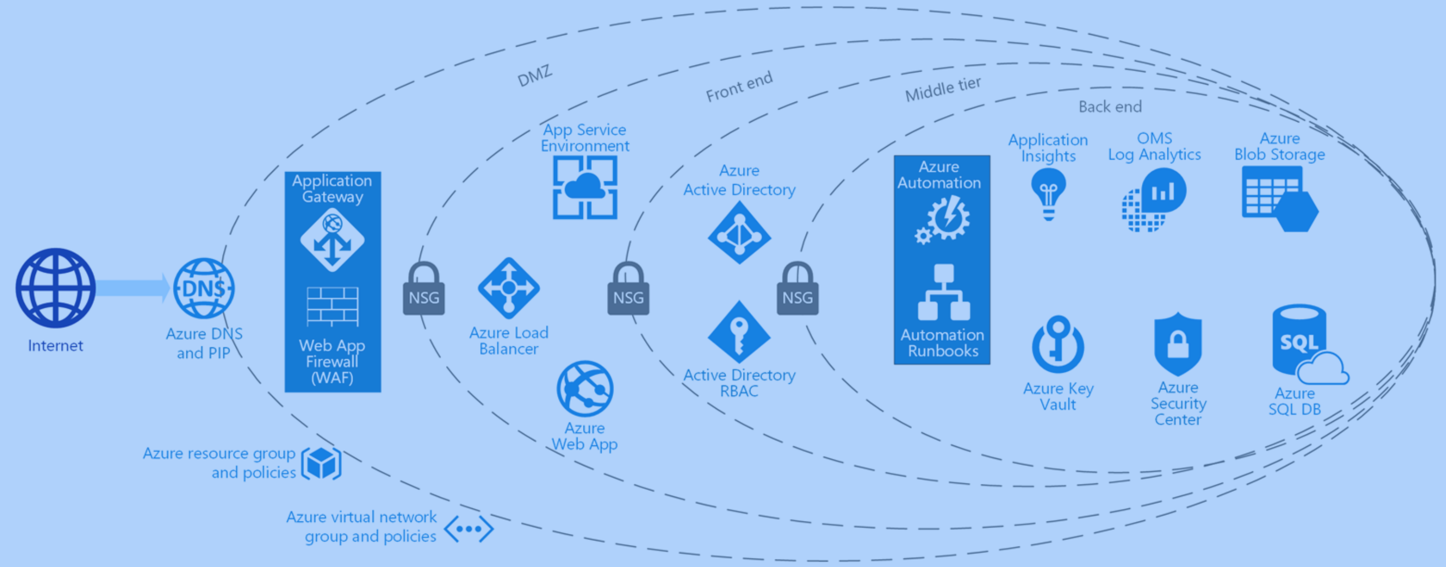
- Operational excellence
- Security
- Performance efficiency
- Reliability
- Cost optimization
- Sustainability

6 pillars of the WAF

Azure

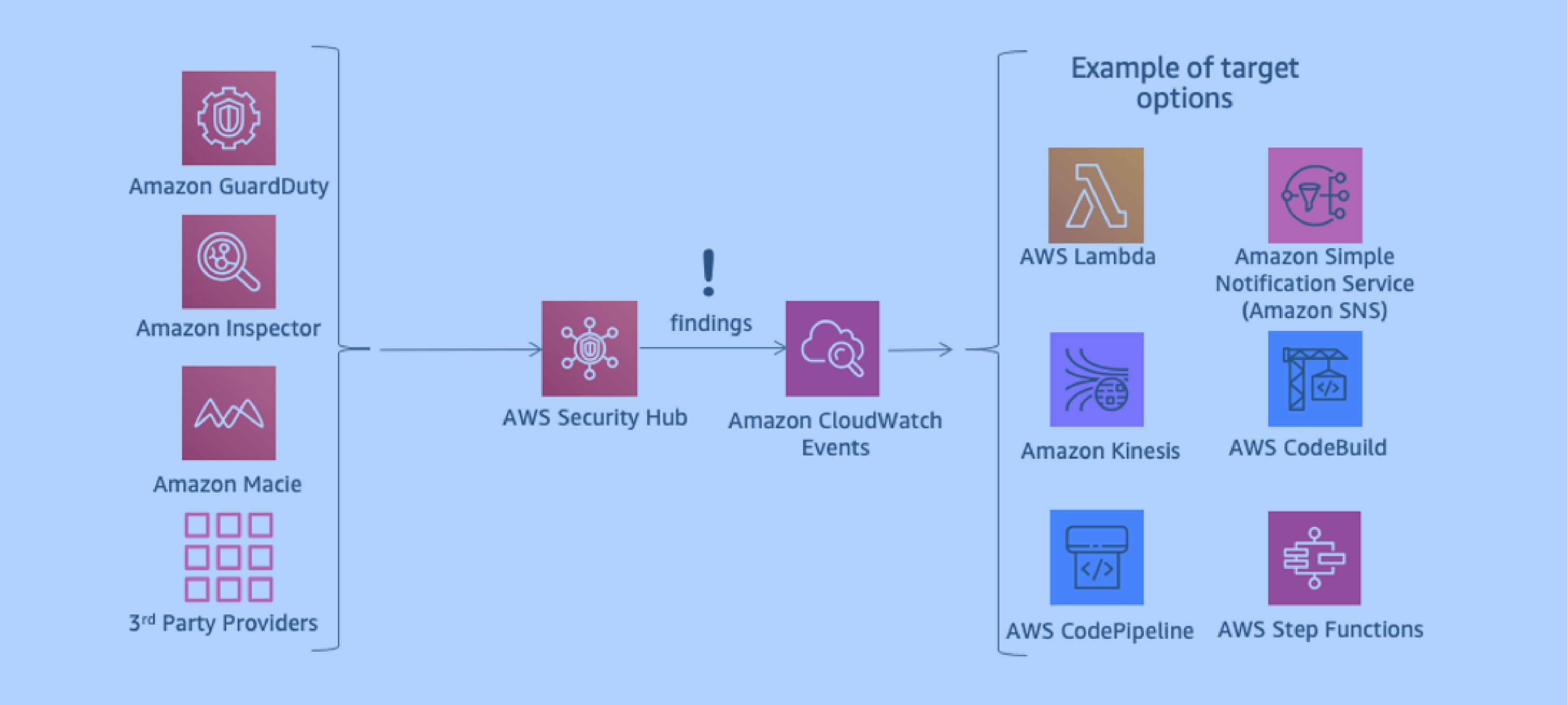
Well-Architected Framework

Security and compliance for regulations



Follow these principles:

- ✓ Document solution Architecture
- ✓ Segment network and solution components
- ✓ Implement zero trust security controls
- ✓ Limit access
- ✓ Ensure disaster recovery and backups
- ✓ Automate processes
- ✓ Monitor and alert



AWS

Well-Architected Framework

Securing and automating compliance

Follow these principles:

- ✓ Automate the collection of compliance information and data
- ✓ Implement automated security and compliance check procedures
- ✓ Automate the remediation of security and compliance issues
- ✓ Secure and automate compliance in a multi-account strategy
- ✓ Automate systems recovery after failure
- ✓ Control access and data
- ✓ Monitor

Mapping infrastructure best practices with DORA

OPERATIONAL EXCELLENCE

- ICT Risk Management
- Monitoring Systems Testing
- Third-Party Risk Management

SECURITY

- Incident Reporting
- ICT Risk Management
- Information Sharing
- Governance and Oversight

PERFORMANCE EFFICIENCY

- ICT Risk Management
- Digital Operational Resilience Testing

RELIABILITY

- ICT Risk Management
- Digital Operational Resilience Testing
- ICT Business Continuity
- Resilience in Critical Services

SUSTAINABILITY

- ICT Risk Management
- Information Sharing
- Governance and Oversight

COSTS OPTIMIZATION

- ICT Risk Management
- ICT Business Continuity
- Governance and Oversight

baltic amadeus

Network Infrastructure: DORA compliance

ICT Risk Management

✓ **Redundancy**
Redundant network paths ensures continuous availability, reduce risks of network failure

✓ **Monitoring**
Helps in the early detection of network issues, supporting proactive risk management

Reliability, Operational excellence

Incident Reporting

✓ **Segmentation**
Isolation of solution components (like front-end, middleware and databases) ensures solution security, facilitates containment of incidents, aiding in accurate and timely reporting

Security

Digital Operational Resilience Testing

✓ **Redundancy testing**
Regular testing of redundant paths to ensure effectiveness

✓ **Monitoring systems testing**
Ensuring monitoring systems are functioning correctly and automated alerting is in place

Reliability, Operational excellence

Storage Infrastructure: DORA compliance

ICT Risk Management

✓ **Data Replication**
Protects against data loss and supports risk management by ensuring data availability

✓ **Backups**
Regular backups are crucial for recovering from incidents

Reliability

Incident Reporting

✓ **Data Integrity**
Helps in ensuring accurate incident reporting by maintaining data accuracy

Security

ICT Business Continuity

✓ **Replicated Storage**
Ensures data is available during a disruption, supporting business continuity

✓ **Backup Systems**
Critical for restoring operations after an incident and data loss

Reliability

baltic amadeus

Compute Infrastructure: DORA compliance

ICT Risk Management

- ✓ **Scalability**
  Supports risk management by handling variable workloads without failure
- ✓ **Load Balancing**
  Prevents server overload, reducing the risk of downtime
- ✓ **Monitoring**
  Monitoring tools letting to track where the data comes from and where it is stored (track information flow and compliance)

Reliability, Performance Efficiency

Digital Operational Resilience Testing

- ✓ **Failover Systems Testing**
  Ensuring failover mechanisms are effective and working correctly
- ✓ **Scalability Testing**
  Regular testing to handle peak loads and identify potential issues

Reliability, Performance Efficiency

ICT Business Continuity

- ✓ **Failover Systems**
  Ensures critical operations continue during server failures
- ✓ **Load Balancing**
  Helps maintain service availability during disruptions

Reliability

baltic amadeus

Security Infrastructure: DORA compliance

ICT Risk Management

✓ **Threat Detection**
Continuous monitoring to identify and mitigate risks

✓ **Access Controls**
Prevent unauthorized access, reducing risk

✓ **ICT Asset inventory**
Identify and manage assets and services

Security, Operational excellence

Incident Reporting

✓ **Incident Response**
Effective incident response plans ensure timely and accurate reporting

Security

Information Sharing

✓ **Threat Detection**
Sharing threat intelligence with other entities to enhance overall resilience

Security

Governance and Oversight

✓ **Access Controls**
Ensures compliance with governance requirements for security

✓ **Incident Response Plans**
Demonstrates oversight in managing and responding to security incidents

Security, Operational excellence

Other Infrastructure controls: DORA compliance

ICT Risk Management

✓ **Cost-effective Solutions**
Implement cost-effective solutions for ICT operations to manage financial risks effectively

Cost optimization, Sustainability

ICT Business Continuity

✓ **Resource Optimization**
Optimize resource usage to minimize costs and ensure continuity of operations during disruptions

Cost optimization, Sustainability

Information Sharing

✓ **Knowledge Sharing**
Share best practices and innovations in sustainable ICT operations to enhance overall resilience and compliance

Cost optimization, Sustainability

Governance and Oversight

✓ **Cost Management Governance**
Establish governance mechanisms to monitor and control ICT costs

Cost optimization, Sustainability

baltic amadeus

Architecture best practices for compliance

STEP 1
Understand DORA, identify stakeholders

STEP 2
Map out the business processes impacted by DORA

STEP 3
Define related data and applications to support DORA

STEP 4
Identify the technology infrastructure needed to meet DORA requirements

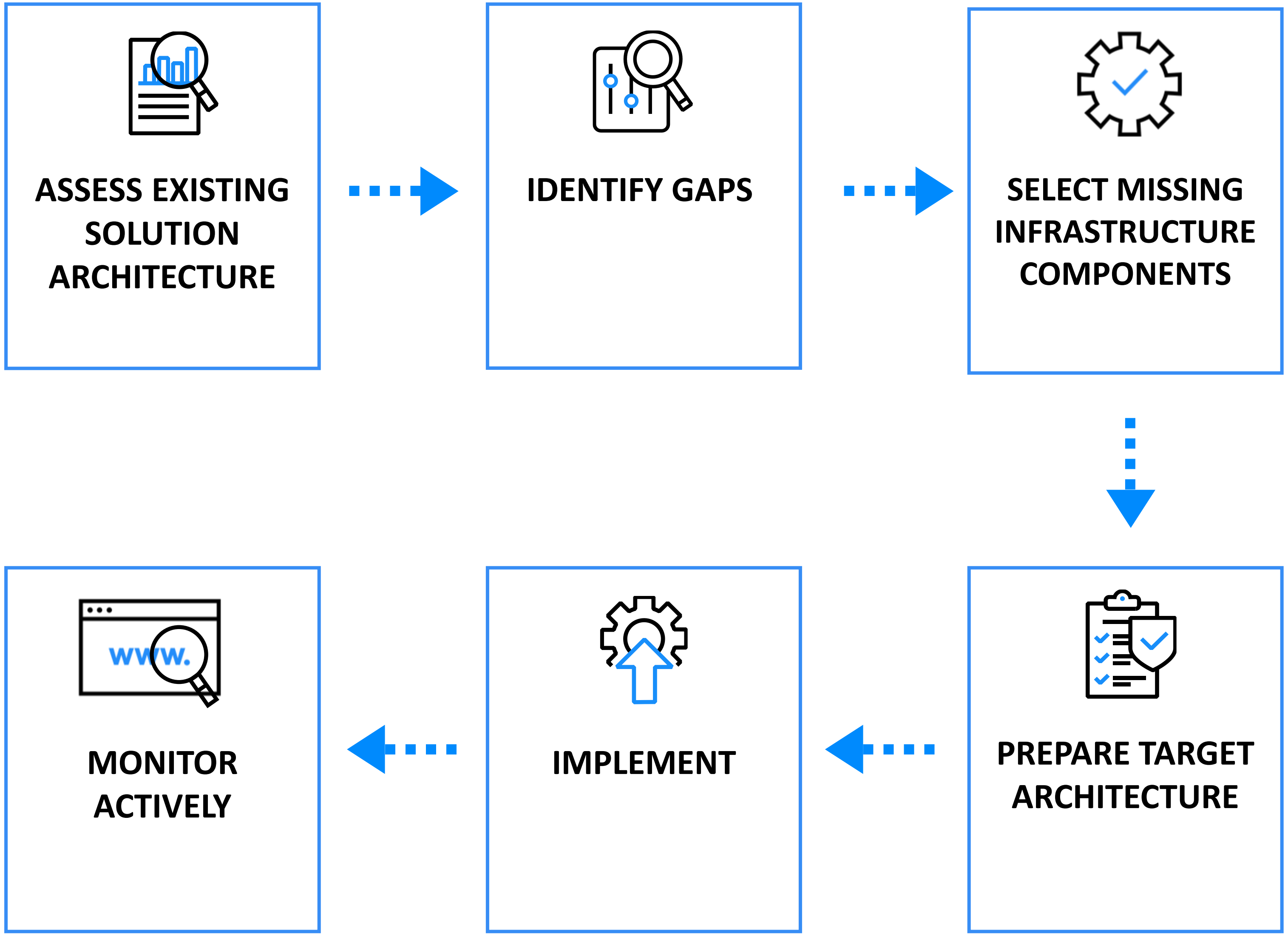
STEP 5
Develop a roadmap for implementation

STEP 6
Plan the transition from the current state to the target business architecture

STEP 7
Monitor the implementation of components and processes to ensure compliance

baltic amadeus

Prepare IT solutions for DORA



ASSESS EXISTING SOLUTION ARCHITECTURE

IDENTIFY GAPS

SELECT MISSING INFRASTRUCTURE COMPONENTS

PREPARE TARGET ARCHITECTURE

IMPLEMENT

MONITOR ACTIVELY

Aligned infrastructure architecture will support Your IT for DORA

Let’s discuss

it further

baltic amadeus

Let’s discuss it further

NERIJUS PAŽERECKAS

HEAD OF ARCHITECTURE

☎ +370 642 22203

✉ n.pazereckas@ba.lt

in Nerijus Pazereckas