FAI COMPLY
COMPLIANCE
CAFE

WELCOME TO

DORA DECODED

DIGITAL RESILIENCE IN PRACTICE

MEET OUR PANEL

Anastasia Kyriacou Petallidou
Compliance Professional

FAI Comply

FAI COMPLY

Panayiotis Varnava, MSc, CISA
Auditor & Cheif Information Security Officer

Konkrit Solutions

KONKRIT SOLUTIONS

Constantinos Koumides
Founder & Director
Cybersecurity & Privacy Advisor
ICON Advisory
President @ ISACA Cyprus

ICON ADVISORY

Kyriacos Kyriacou
Co-Founder & Solutions Director

Ralliton

Ralliton

DORA: ONE YEAR ON

From Implementation to Operational Maturity

DORA: ONE YEAR ON

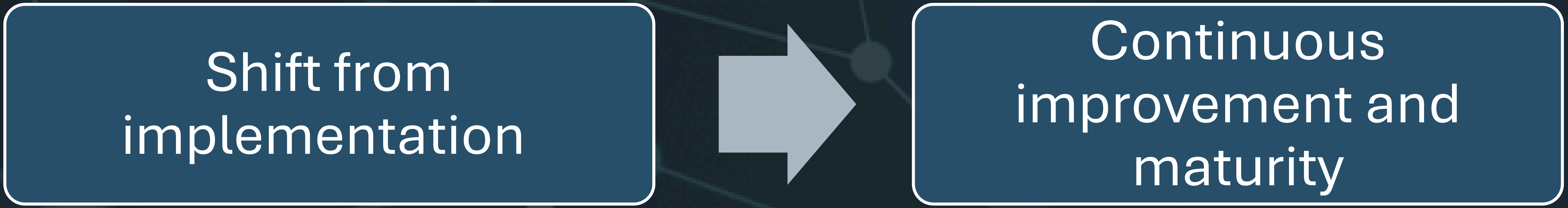
FROM IMPLEMENTATION TO OPERATIONAL MATURITY

DORA ONE YEAR ON: WHERE WE STAND

- Regulation in force since 17 January 2025
- CySEC now shifting to active supervision & enforcement
- Initial audits show gaps between policy readiness and operational execution
- Industry still adjusting to new reporting and testing obligations

EVOLVING FRAMEWORK & REGULATORY FOCUS

- ESAs issuing clarifications and FAQs
- CySEC applying DORA principles in onsite reviews
- Early enforcement emerging across EU



Shift from implementation

Continuous improvement and maturity

THE CORE PILLARS OF DORA

Pillar 1: ICT Risk Management – Build and maintain secure, resilient systems

Pillar 2: Incident Reporting – Detect, classify, and report major ICT incidents

Pillar 3: Resilience Testing – Test systems regularly to ensure robustness

Pillar 4: Third-Party Risk – Manage risks from outsourced ICT services

Pillar 5: Information Sharing – Share cyber-threat intelligence responsibly

THE PROPORTIONALITY PRINCIPLE

“DORA is established based on the principle of proportionality considering the size, overall risk profile, and the nature and complexity of the financial entities’ services, activities, and operations..”

PROPORTIONALITY PRINCIPLE

- Explicit exemptions for microenterprises
- Simplified ICT risk management for small and non-interconnected investment firms
- Exemptions for smaller entities from weekend reporting
- Only major ICT-related incidents are reported
- ICT systems, protocols and tools appropriate to the magnitude and impact of operations

PILLAR ONE: ICT RISK MANAGEMENT

Financial entities should have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively.

ICT RISK MANAGEMENT

Governance & Accountability

- The management body (Board) bears ultimate responsibility
- Clear, and roles, responsibilities and reporting lines.

ICT Risk Framework

- Must include at least strategies, policies, procedures, protocols, and tools
- Include a digital operational resilience strategy

ICT Systems, Protocols & Tools

- Should be reliable, secure, and regularly updated
- Defence-in-depth measures
- Focus on maintaining confidentiality, integrity, and availability (CIA)

ICT RISK MANAGEMENT

Identification & Classification

- Identify critical ICT assets, functions, and dependencies
- “Register of Information”
- Classify ICT risks and assets based on their business criticality

Protection & Prevention

- Establish preventive security and protection measures
- Apply multi-layered security controls appropriate to identified risks.
- Regularly review and update

Detection & Monitoring

- Implement mechanisms to detect anomalous ICT activities or security breaches.
- Promptly log, analyse, and escalate detected events

ICT RISK MANAGEMENT

Response & Recovery

- Develop incident response and recovery plans.
- Plans must define recovery time and recovery point objectives.
- Ensure restoration of normal operations and report incidents

Back Up & Recovery Policies

- Maintain secure and tested backups of critical systems and data.
- Ensure backups are geographically dispersed.
- Test restoration procedures regularly.

Learning & Evolving

- After each incident, entities must analyse root causes and implement corrective actions.
- Continuous improvement of ICT frameworks is required.
- Lessons learned should be integrated into training and policy updates.

SUMMARY: ARTICLES 5-14

- Have a **board-approved ICT risk management framework**
- Maintain **secure, resilient ICT systems**
- **Continuously monitor** and **test** them
- Be able to **respond**, **recover**, and **learn** from ICT incidents
- **Manage ICT third-party risks** effectively

STRENGTHENING ICT RISK MANAGEMENT

- Risk assessments must reflect real ICT architecture
- Need for complete, accurate asset inventories (still a major gap)
- Board reporting must be meaningful, not technical jargon
- Risk appetite and thresholds must be measurable
- Firms still struggle with mapping dependencies and critical functions

PILLAR TWO: INCIDENT REPORTING

DORA mandates that firms detect, classify, and report major ICT-related incidents to their relevant authority within strict timeframes.

This includes detailed root-cause analyses, impact assessments, and follow-up reports.

MAJOR IT INCIDENT

Service downtime

Large client impact

Data loss, corruption, or confidentiality breach

Financial loss or economic impact

Systemic risk

Significant degradation

If thresholds are met → **reporting becomes mandatory**

INTERNAL PROCESSES REQUIRED

- Incident detection and monitoring tools feed directly into the reporting workflow
- Internal incident registers are maintained
- Staff know when and how to escalate incidents internally
- Reporting deadlines are understood and achievable
- Coordination between ICT, Risk, Compliance, and Management

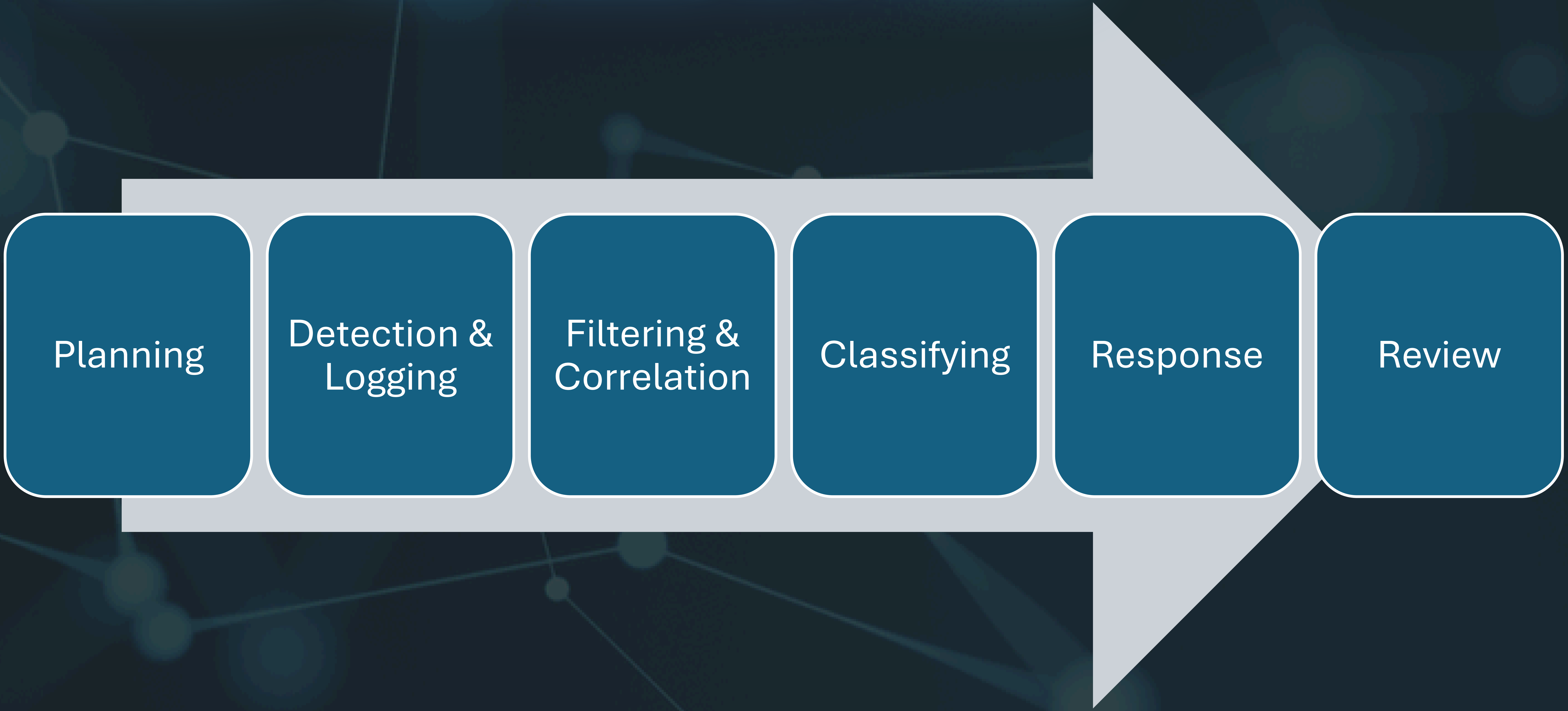
INCIDENT CLASSIFICATION & REPORTING

- Firms still over-reporting or under-reporting
- Incident classification methodologies often untested
- Reporting timelines require pre-defined playbooks
- Logs & monitoring insufficient for real-time detection
- Communication between ICT & business units often weak

PILLAR THREE: DIGITAL OPERATIONAL RESILIENCE TESTING

Firms must regularly test the strength of their ICT systems and cybersecurity measures. This includes vulnerability assessments and penetration testing, scenario-based testing and Advanced Threat-Led Penetration Testing (TLPT) for larger or critical entities.

SECURITY MONITORING IN 6 STAGES



Planning

Detection & Logging

Filtering & Correlation

Classifying

Response

Review

TESTING GOVERNANCE

- Tests must be planned, risk-based, and approved by senior management.
- Results must feed directly into ICT risk assessments, incident response enhancements and backup & recovery improvements, as well as training needs
- Weaknesses must be tracked, prioritised, and remediated.
- All testing evidence must be kept for supervisory review (e.g., CySEC)

RESILIENCE TESTING ONE YEAR ON

- Firms now required to produce testing evidence
- Scenario-based testing expected annually
- Pen testing frequency must match risk profile
- Testing results must be fed back into risk assessments
- Supervisors may question unrealistic or shallow tests

PILLAR FOUR: ICT THIRD PARTY RISK

DORA introduces strict oversight of outsourced ICT services, requiring firms to assess, monitor, and manage risks arising from third-party providers such as cloud, data, and software vendors.

IDENTIFICATION & OVERSIGHT

- Maintain a complete register of all ICT third-party providers and outsourced functions.
- Classify providers based on criticality and dependency level.
- Monitor provider performance, SLAs, and resilience capabilities.
- Assess concentration risk (e.g., reliance on single provider or cloud region).

MANDATORY CONTRACT ELEMENTS

Service levels, uptime, support, and reporting obligations

Access, audit, and inspection rights

Security and incident management provisions

Data protection, encryption, and exit/termination conditions

CTTPS, EXIT STRATEGIES & RESILIENCE

Critical ICT Third-Party Providers (CTPPs)

- Certain providers may be designated “critical” by EU authorities.
- They will be subject to **direct oversight** by ESA-led supervisory bodies.
- Firms must ensure arrangements allow compliance with those rules.

Exit & Continuity Planning

- Maintain **tested exit strategies** for key ICT services.
- Ensure business continuity and disaster recovery considerations extend to third-party providers.
- Be able to **switch providers or bring services in-house** if required.

THIRD-PARTY OVERSIGHT REALITIES

- Contract gaps remain widespread
- Mandatory DORA clauses often missing from legacy agreements
- Lack of audit rights over cloud providers
- Weak exit strategies and inadequate subcontracting visibility
- Concentration risk assessments not updated since 2024

PILLAR FIVE: INFORMATION & INTELLIGENCE SHARING

Financial entities are encouraged to share cyber-threat intelligence—including indicators of compromise, vulnerabilities, attack techniques, and lessons learned—through trusted and secure information-sharing arrangements.

WHAT CAN BE SHARED?

- Cyber threat intelligence
- Indicators of compromise (IOCs)
- TTPs (tactics, techniques, procedures) used by attackers
- Vulnerabilities and exploitation patterns
- Lessons learned from ICT incidents
- Best practices for prevention and response

REQUIREMENTS & SAFEGUARDS

- Sharing must occur within trusted communities or information-sharing arrangements.
- Arrangements must protect Confidentiality, Data protection and GDPR compliance, as well as security of the exchanged information.
- Firms must ensure sharing does not create competitive or market risks.
- Information must be actionable, helping firms detect or prevent threats.

CORE COMPLIANCE EXPECTATIONS IN PRACTICE

- Firms must now demonstrate compliance, not just document it
- Evidence-based supervision: logs, testing results, incident metrics, contract audits
- Focus on governance quality and board oversight
- Realistic and frequent testing
- Integrating DORA controls into business-as-usual processes
- Mature outsourcing governance
- Closing gaps identified during internal reviews

WHERE CYPRIOT FIRMS STILL STRUGGLE

- Incomplete asset inventories
- Manual monitoring with limited automation
- Vendor contracts without DORA clauses
- Limited documentation of resilience tests
- Weak KRIs/KPIs for ICT risk

ACTION PLAN FOR 2025–2026

1. **Conduct a DORA “one year on” health check**
2. **Improve asset inventories and ICT architecture mapping**
3. **Strengthen incident classification and reporting rehearsals**
4. **Review and update all ICT third-party contracts**
5. **Increase testing sophistication**
6. **Implement dashboards for board oversight**
7. **Build readiness for potential TLPT designation**

FINAL TAKEAWAYS

- One year on, DORA is entering its real supervisory phase
- Firms must now show functioning processes and evidence
- CySEC is raising expectations for maturity
- Early investment in operational resilience pays off
- The next 12 months will define long-term compliance posture

FAI COMPLY
COMPLIANCE
CAFE

DORA DECODED

DIGITAL RESILIENCE IN PRACTICE

THANK YOU FOR ATTENDING