DORA

Implementation and Challenges

C'EST VOUS L'AVENIR SOCIETE GENERALE

AGENDA

1. Why has Resilience become a strategic topic?
2. A key Program of the Bank
3. The DORA project within SG
4. What are the tasks to be planned?
5. What are the challenges we are facing?

THE OPERATIONAL RESILIENCY : A STRATEGICAL TOPIC

- **Cyber threat**
- **Geopolitical tensions**
- **A more demanding digital world**
- **Supervisors focus**

In this context, the Bank Senior Management wants to ensure the financial core (essential) activities can survive plausible extreme crisis

A PROGRAM MODE APPROACH

- **Capacity to manage crisis : Business Continuity Management tooling and resources**
- **Capacity to survive during the first phasis of the crisis : find non or degraded IT solutions sometimes**
- **Capacity to reconstruct in an acceptable time frame : shorten the systems' rebuilding and adopt a resilient by design approach**

DORA is naturally a dedicated project within this program (strong links as DORA requires to identify key activities and to review testing and third parties monitoring)

THE DORA PROJECT ORGANIZATION

- **Governance**
  - Sponsorship : global program, Deputy CEO and, as for the DORA project : the Group CIO
  - Key stakeholders of the DORA Steering Committee : the Business CIOs, the Group Operational Risk Head and the CISO
  - A transversal project team relying on local (entities and subsidiairies) or Business Units points of contact or project managers, while interacting with Legal and Risk functions
- **An approach which copies / pastes the chapter of the Regulation with 4 sub streams at this stage :**
  - ICT risk framework
  - Incident reporting
  - Testing policy
  - IT Third Parties

Diagnosis on policies/norms and corresponding operational gaps : we are not starting from scratch though. After this diagnosis, we will build the detailed roadmap with the IT Departments, the Infrastructure and the Entities in liaison with the Risk function.

THE NATURE OF THE TASKS IDENTIFIED

- **Normative gaps :**
  - Define and formalize the Bank digital operational resilience strategy
  - Update the existing policies : Group Information System Security Policy, RCSA, Incidents reporting and audits plans
  - Write data backup policies / procedures and recovery methods
  - Define digital operational resilience testing program
  - Update contractual clauses related to third Parties including the exit strategy and associated operational procedures
- **Operational gaps :**
  - Identify for all business functions and crucial processes with their related ICT assets and Third Parties, huge work on referential
  - Complement the existing tests with new resiliency ones and perform penetration testing every 3 years
  - Involve Management Body at the right level
  - Implement a new monitoring approach of our IT suppliers

At this stage, we have identified 108 entities, 44 normative workloads and 182 operational gaps. We plan finishing the diagniosis on gap in H2 and start the execution phasis in September 2023.

CHALLENGES

- **Timeline and normative requirements' interpretation : several RTS have not been published and we have to begin**
- **Scope of entities : how can we rely on the proportionality principle**
- **Efforts on referential, IT Third parties' management and testing**
- **A question mark on the level of preparation within the Third Parties community**
- **And classical challenge on budget and key experts' resources**

One mitigation to make sure we are not following wrong paths: link with Supervisors and creation of a « groupe de place »