IMPACT

Cyber Security Status Update and Defense Strategy

Executive summary by Potech Consulting covering security assessments and suggested action plan

June 2021

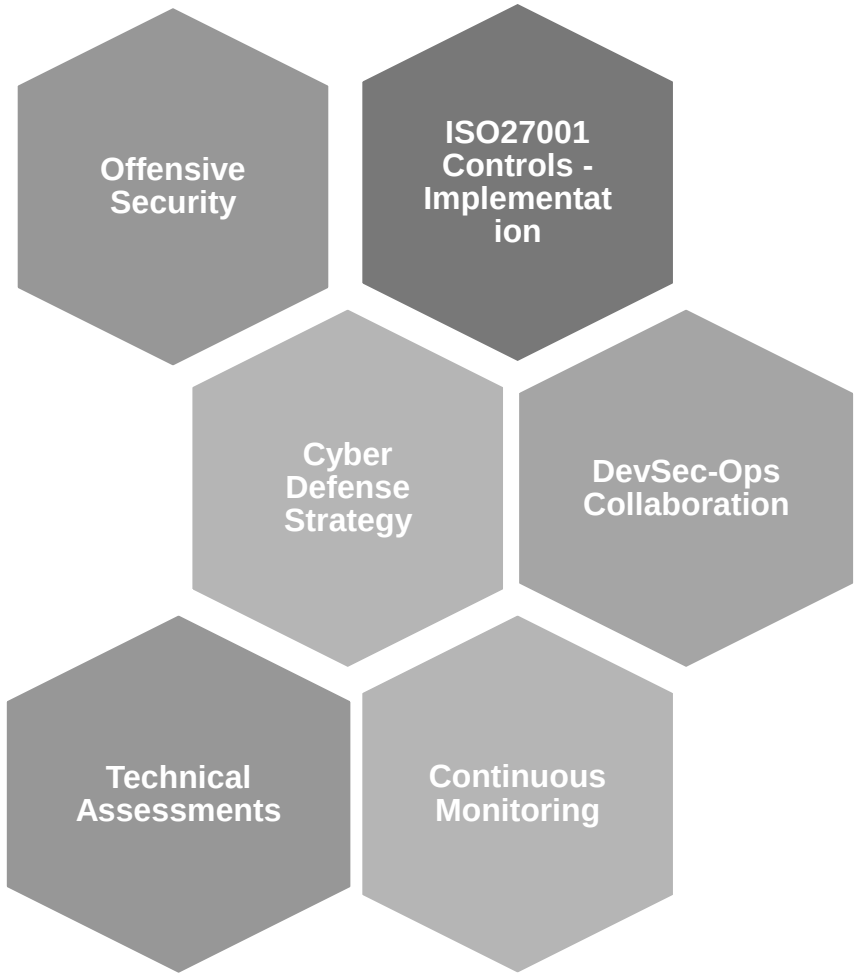
Cyber Defense Strategy

Cyber-Defense Strategy

The results showcased in this executive report are based on the technical security assessments conducted by Potech Consulting until June 2021.

An advanced defense strategy has been put in place according to Potech Consulting's suggested action plan:

- Offensive Security (Quick win)
  - Penetration tests
  - Red Team Exercises
- Technical Assessments
  - IT Infrastructure Review
  - Database Security Assessments
- Information security standard enforcement ISO27001
  - User Access Management
  - Policy/Process Enforcement, KPI KRI Definition
  - Hardening Procedures
- DevSec-Ops Execution and Collaboration
- Advanced Monitoring



IMPACT

Cyber Security Status Update

1- Technical Assessments:

- Exposed Servers and application testing - Continuous
  - ✓2 **Critical** risks were detected and resolved immediately
  - ✓7 **High** risks: 3 resolved and under deployment - 2 resolved - 2 partially solved/mitigated
  - ✓11 **Medium** risks: 3 solved and deployed on live – remaining remediations ongoing progressively
  - ✓3 **Low** risk
- Compromise Assessment – Running
  - ✓ covax.moph.gov.lb - Done: no compromise
  - ✓ covid.pcm.ogv.lb – Scheduled
  - ✓ cp.cib.gov.lb - Scheduled

2- Security Checklist as per ISO27001 - Running
- IT / Data Security Infrastructure Review - Done
- User access management - Done
- Password management - Running
- Segregation of duties - Done
- Application/Database security review and Hardening - Running
- Log management - Scheduled
- Business Continuity Plan and Drills - Scheduled

3- Policies and Processes Review and Improvement - Running
- Change and incident management – Policies done
- HR management – Policy done
- Access management – Policy done
- Backup management – Policy done
- Secure –SDLC – Running
- IT acquisition and password management – Policies done
- IT service continuity management – Scheduled
- Release management – Scheduled
- Service asset and configuration management – Scheduled

IMPACT

Compromise Assessment

Compromise Assessment Scenarios

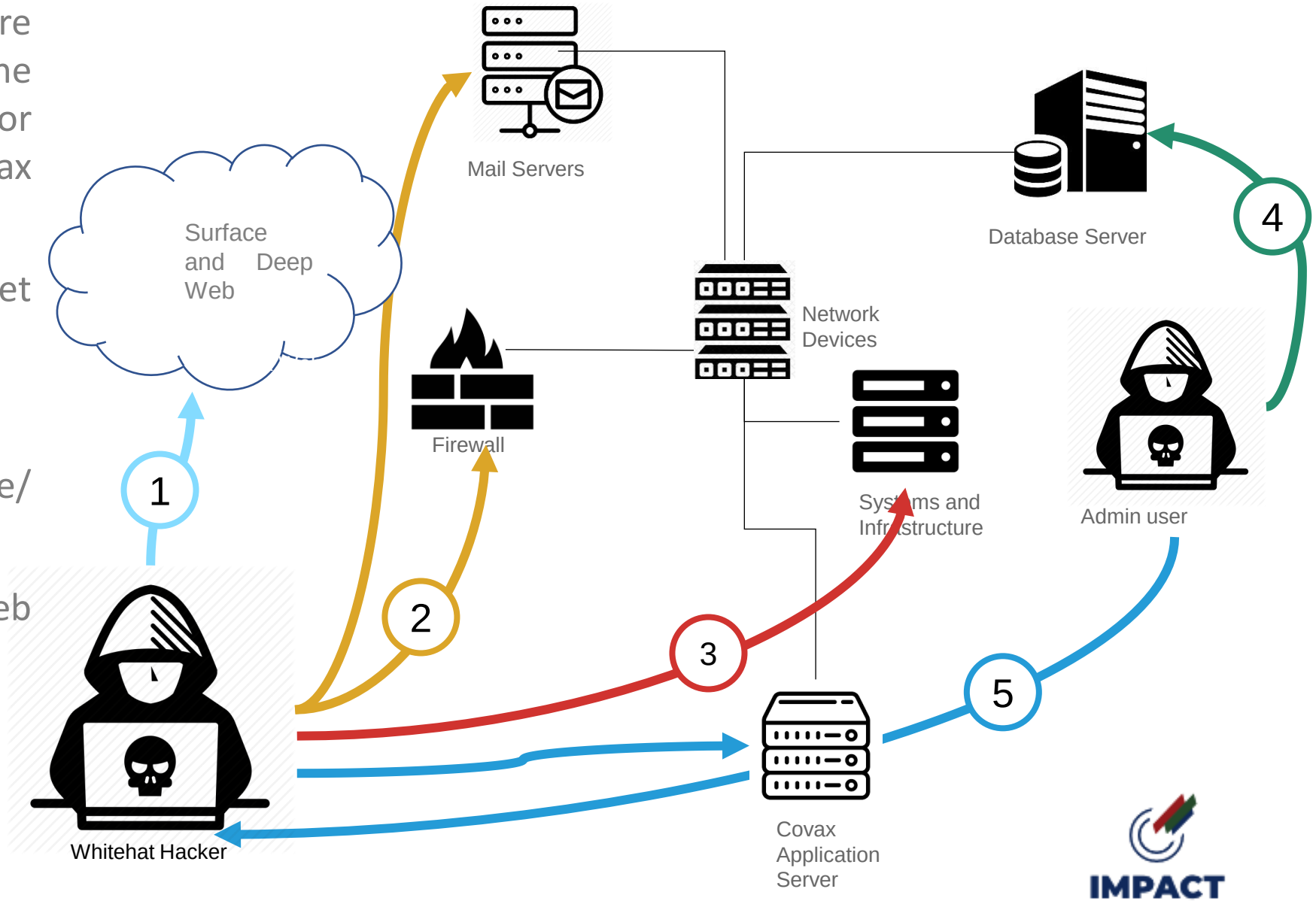
The worst-case scenarios were assumed when conducting the exercise, and were examined for elimination or validation (covax server) :

External attacker on internet perimeter

1. Passive data extraction
2. System Compromise/ Bruteforce attacks
3. Extract PII data through Web application weakeness

Malicious/Compromised Administrator/User (Internal threat)

4. Internal malware/virus
5. Malicious Admin/User



IMPACT

Compromise Assessment Status Update

The following scenarios were assumed (as per previous slide) when conducting the exercise and looked for indicators of compromise:

1. External Attacker On internet Perimeter: 1 2 3
    a. Web application and Injection attacks: Around 10000 attempts, 0 successful attacks
    b. Brute-force attacks: No attempts detected
2. Malicious/Compromised Administrator/User (Internal threat) 4 5
    1. Uploaded/modified Files: no malicious behavior detected
    2. User History Analysis and Activity Logs: no suspicious activity detected
    3. Network Analysis: monitoring is on-going, no suspicious connections detected so far

IMPACT

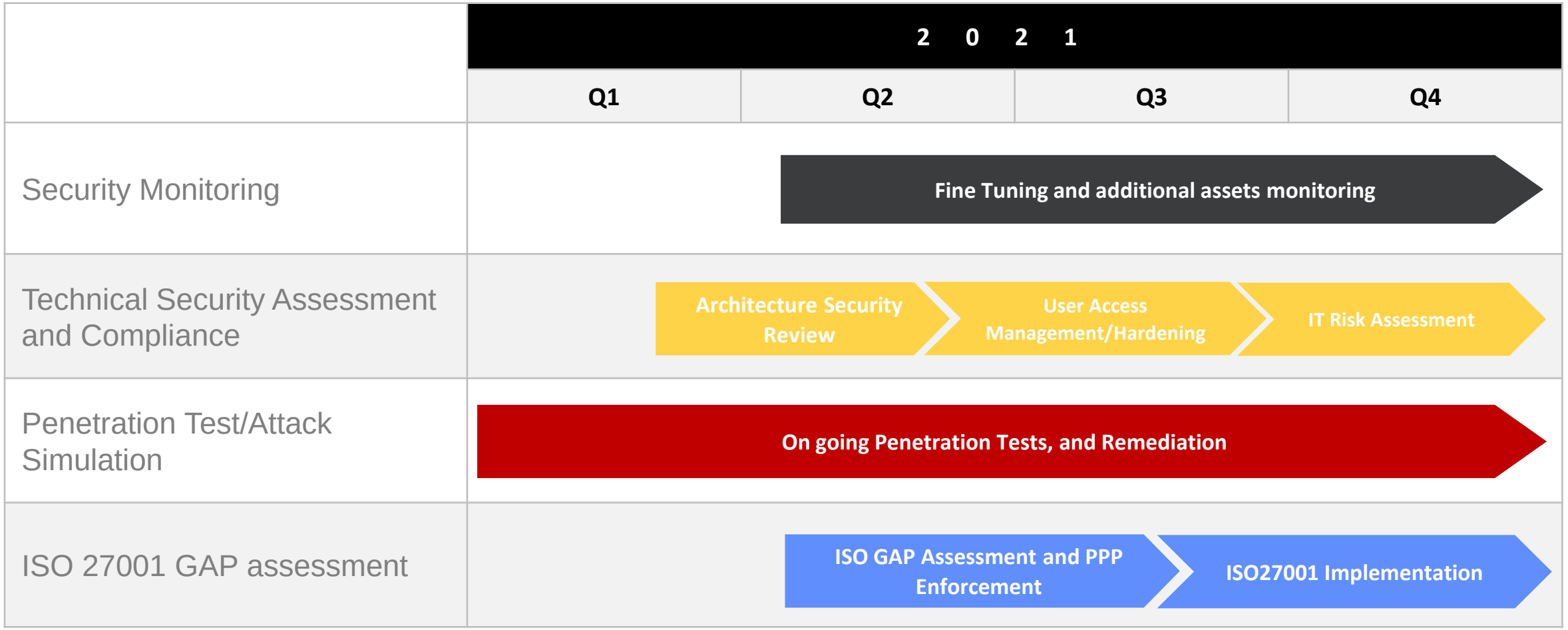
The Way Forward

Progress and Action Plan

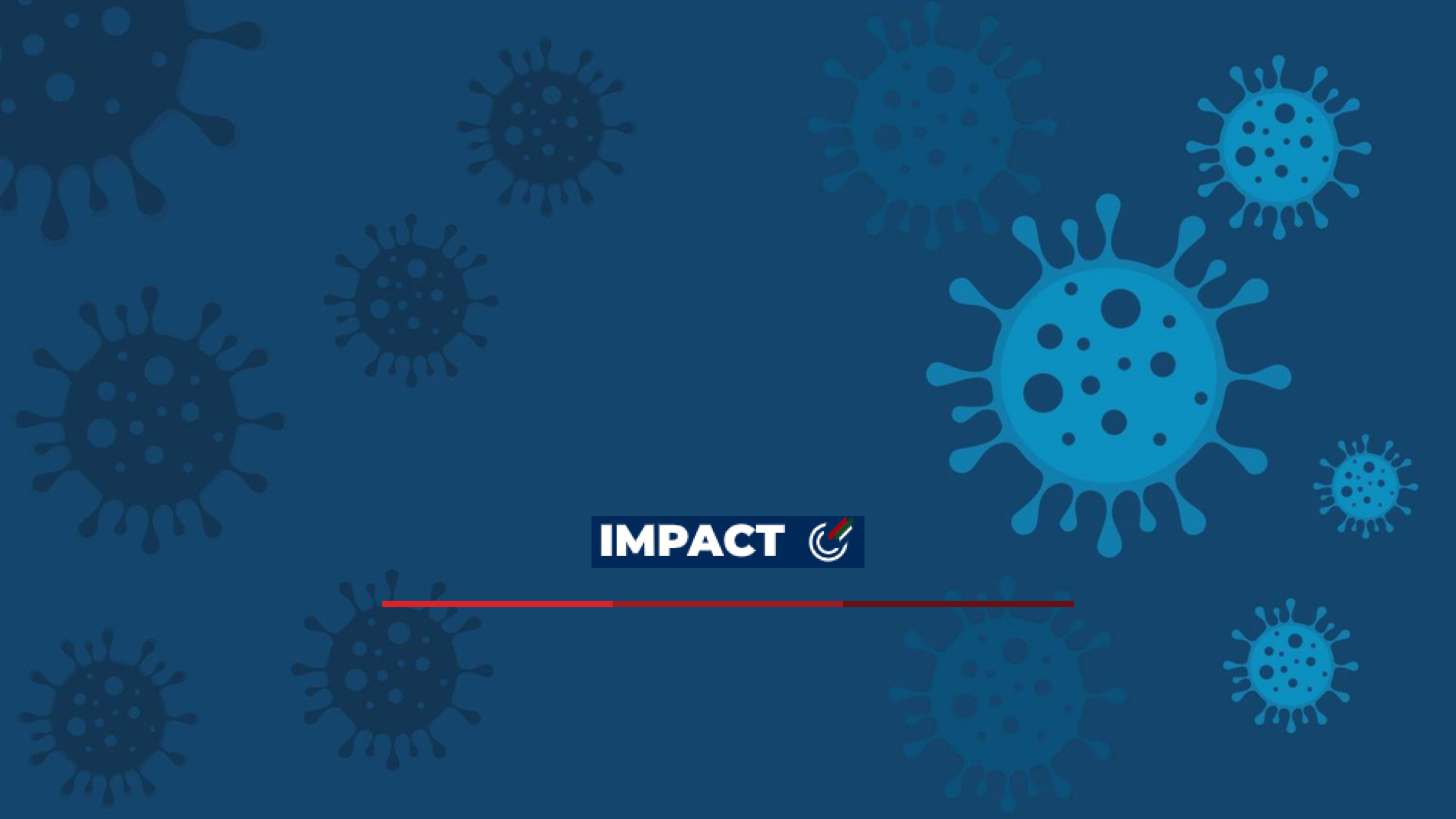
Agenda item	Date/Deadline	Status
Penetration test over Covid Web application (appointment scanner, curfew scanner)	February 2021	Completed
Penetration test over COVAX web application	February 2021	Completed
Penetration test over Impact informational web application	February 2021	Completed
Penetration test over Impact backend/APIs	February 2021	Completed
GB Penetration test over cp web applications	March 2021	Completed
GB Penetration test over dcp web applications	March 2021	Completed
GB Penetration test over cop/crm web applications	March 2021	Completed
Continuous follow-up/retest and fine tuning	Weekly	Ongoing
Compromise Assessment on Impact applications/servers	August 2021	Ongoing
IT infrastructure security review	March 2021	Completed
RedTeam Exercise and Mobile Security	August 2021	Planned
User Access Management Review	April 2021	Ongoing
White Box Application/ Database Security assessment and hardening	May 2021	Ongoing
Review/Development of infosec policies	May 2021	Completed
Review/Development IT/SDLC processes	July 2021	Planned

IMPACT

Roadmap 2021



IMPACT


IMPACT