Security Incident Response Playbook (SOC 2)

1. Objectives

Incident response objectives is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Incident response objectives is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Incident response objectives is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Incident response objectives is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Incident response objectives is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Incident response objectives is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Incident response objectives is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Incident response objectives is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements.

2. Roles and Responsibilities

Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Roles include Incident Commander, Security Lead, Legal, and Communications is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements.

3. Detection and Triage

Security monitoring and triage procedures is a critical component of a regulated banking

platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Security monitoring and triage procedures is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Security monitoring and triage procedures is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Security monitoring and triage procedures is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Security monitoring and triage procedures is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Security monitoring and triage procedures is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Security monitoring and triage procedures is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Security monitoring and triage procedures is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements.

4. Containment and Recovery

Containment, eradication, and recovery activities is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Containment, eradication, and recovery activities is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Containment, eradication, and recovery activities is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Containment, eradication, and recovery activities is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Containment, eradication, and recovery activities is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Containment, eradication, and recovery activities is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Containment, eradication, and recovery activities is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Containment, eradication, and recovery activities is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements.

5. Post-Incident Review

Post-incident review and evidence collection is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Post-incident review and evidence collection is a critical component of a regulated banking platform and must be

designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Post-incident review and evidence collection is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Post-incident review and evidence collection is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Post-incident review and evidence collection is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Post-incident review and evidence collection is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Post-incident review and evidence collection is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements. Post-incident review and evidence collection is a critical component of a regulated banking platform and must be designed, implemented, monitored, and audited in accordance with applicable regulatory, contractual, and internal policy requirements.