infoexpress

EasyNAC

Whitepaper: Achieving **BSP Circular 982 Compliance** with **EasyNAC** for Financial Institutions

Simple Control, Strong Security

www.easynac.com

sales@infoexpress.com | 2975 Bowers Avenue, #323, Santa Clara, CA 95051 USA | Phone: +1 650-678-1541

CONTENTS

Executive Summary

Bangko Sentral Supervised Financial Institutions (BSFIs) face ever-increasing cyber risks amid rapid digital innovation. The BSP Circular No. 982 establishes a comprehensive information security framework that mandates governance, risk management, prevention, detection, response, and resilience measures.

This whitepaper highlights how EasyNAC aligns with BSP 982's requirements, enabling BSFIs to achieve compliance while strengthening their overall cybersecurity posture.

Key Business Benefits:

- **Simplified Compliance:** Automates asset inventory, access control, and reporting to reduce audit preparation time and lower the cost of regulatory compliance.
- **Faster Incident Containment:** Detects and quarantines rogue or non-compliant devices in under **5 seconds**, minimizing potential business disruption.
- **Network-Agnostic Design:** Deploys without changes to existing switches, routers, VLANs, or wireless infrastructure—accelerating time to compliance and reducing project risk.
- **Future-Ready Security:** Extends protection across LAN, WLAN, VPN, IoT, and remote sites using Enforcer Sensors, ensuring scalability as digital operations expand.

EasyNAC combines robust device visibility, compliance enforcement, automated threat response, and rapid incident containment—critical enablers for BSFIs seeking both **regulatory adherence and resilient security against evolving cyber threats**.

EASYNAC

EasyNAC is a **third-generation Network Access Control (NAC) solution** engineered to be simple, secure, and cost-effective. Unlike traditional NAC platforms that require complex switch integration, VLAN redesign, or endpoint reconfiguration, EasyNAC is **agentless by default** and deploys with **no changes to your existing network infrastructure**.

At its core, EasyNAC provides:

- **Comprehensive Visibility:** Automatically discovers and inventories every device—corporate, BYOD, guest, IoT, or rogue—the moment it connects to the LAN, WLAN, or VPN.
- **Access Control Without Complexity:** Enforces baseline security and role-based access, ensuring only trusted and compliant devices gain entry.
- **Regulatory Compliance by Design:** Verifies Active Directory membership, anti-virus and patch status, and other compliance criteria before allowing network access.
- **Rapid Incident Containment:** Detects and quarantines unauthorized or infected devices in under **5 seconds**, reducing risk of malware spread or data loss.

- **Seamless Integration:** Works with firewalls, XDR, SIEM, MDM, and other security systems to automate threat response and support layered defense.

EasyNAC also includes advanced features such as **MAC spoofing protection, deception-based hacking detection, and automated remediation options**. For distributed BFSIs, it extends coverage to branches and remote sites through lightweight **Enforcer Sensors**, ensuring enterprise-wide protection without costly WAN redesigns.

By combining **simplicity of deployment** with **Zero Trust enforcement and advanced threat response**, EasyNAC delivers a NAC solution that aligns with BSP Circular 982 while remaining practical, scalable, and resilient for financial institutions of all sizes.

INTRODUCTION

The financial industry faces unprecedented risks from cyberattacks, insider threats, and regulatory scrutiny. Bangko Sentral ng Pilipinas (BSP) has responded with Circular 982, which defines mandatory information security management practices tailored to the complexity and risk profile of each supervised financial institution.

Circular 982 requires BSFIs to safeguard the **confidentiality, integrity, and availability** of information assets through proactive governance, risk-based controls, and continuous improvement. For many organizations, meeting these requirements poses challenges—particularly where legacy systems, complex networks, and resource limitations complicate compliance efforts.

EasyNAC addresses these challenges by providing a **network-agnostic, agentless Network Access Control (NAC) solution** that delivers strong security without requiring network changes, VLAN redesigns, or costly infrastructure upgrades. By automating device discovery, enforcing access policies, and integrating with existing security tools, EasyNAC enables BSFIs to align with BSP 982 while simultaneously improving operational resilience.

With its holistic approach, EasyNAC empowers BSFIs to:

- Secure information assets against unauthorized access and advanced threats.
- Manage risks dynamically through continuous visibility and compliance monitoring.
- Support governance and audit requirements with detailed, real-time reporting.

In short, EasyNAC makes compliance with BSP 982 not just achievable—but a catalyst for stronger cybersecurity and improved trust with regulators, customers, and stakeholders.

BSP Circular 982 Overview

Policy Objective: Safeguard confidentiality, integrity, and availability of BSFI information assets.

Key Areas: Information security governance, risk management, preventive controls, detection, response, recovery, and continuous improvement.

IT Profiles: Simple, Moderate, and Complex classifications define required security maturity levels.

Mapping BSP Controls to EasyNAC Capabilities

ASSET IDENTIFICATION AND ACCESS MANAGEMENT

Control (Section 3.2, Identification Phase in ISP Management):

Maintain an up-to-date inventory of all information system assets including hardware, software, users and their access rights; monitor configuration changes and unauthorized access.

EasyNAC Response:

- Automated discovery and real-time inventory of devices and users connected to the network.
- Access control based on device compliance and user role, with continuous posture assessment.
- Detection and alerting on unauthorized devices or configuration changes.

IDENTITY AND ACCESS MANAGEMENT

Control (Section 3.3.3.2, Identity and Access Management):

Enforce least privilege principle, periodic user access reviews, approval workflows for access changes, and multi-factor authentication for high-risk transactions.

EasyNAC Response:

- Enforces network access policies reflecting least privilege and role-based access.

NETWORK SECURITY AND SEGMENTATION

Control (Section 3.3.3.3, Network Security):

Establish security zones, implement access policies per zone, monitor cross-domain access, and prevent unauthorized device connections including WLAN.

EasyNAC Response:

- Network segmentation enforced by device compliance and user identity through ACL.
- Real-time monitoring for rogue or unauthorized devices across wired and wireless networks.
- Policy enforcement and automated quarantining.

THREAT DETECTION AND INCIDENT RESPONSE INTEGRATION

Control (Section 3.4 and 3.5, Detection and Response):

Implement layered detection mechanisms including IDS, SIEM integration, and incident response plans with trained responders and forensic readiness.

EasyNAC Response:

- Provides continuous endpoint and layer-2 activity monitoring for anomaly detection.
- Automated quarantine of compromised or out-of-compliance devices.
- Integration with SIEM, Firewall, and other network security devices and other and incident workflows for rapid response by dynamically isolating or restricting device access.

SECURITY POLICY COMPLIANCE AND AWARENESS

Control (Section 3.3.1, Administrative Controls):

Develop and enforce comprehensive security policies, standards, and conduct regular employee security awareness and training.

EasyNAC Response:

- Enforces policy compliance through automated network access controls.
- Generates compliance reports for policy enforcement verification.

PATCH MANAGEMENT AND CHANGE CONTROL

Control (Section 3.3.3.8.3 and 3.3.3.8.2, Patch Management and Change Management):

Promptly apply security patches to systems and control IT environment changes through documented processes and approvals.

EasyNAC Response:

- Monitors device compliance status including patch levels via integration module before granting network access.

REMOTE ACCESS SECURITY

Control (Section 3.3.3.2.1, Remote Access):

Allow remote access only with formal authorization, risk-based authentication, and secure communication channels with logging and monitoring.

EasyNAC Response:

- Controls and authenticates all devices connecting remotely, ensuring policy compliance.
- Least Privilege Access principles applied to VPN users

CONTINUOUS TESTING AND IMPROVEMENT

Control (Section 3.7, Assurance and Testing):

Conduct continuous testing including vulnerability assessments, penetration testing, and scenario-based exercises to validate security control effectiveness.

EasyNAC Response:

- Provides detailed access and compliance logs to support internal audits and penetration tests.
- Enables simulated attack scenarios by dynamically isolating or restricting device access to validate response.

EasyNAC Business Benefits

EasyNAC empowers BSFIs to comply with BSP Circular 982 while delivering measurable improvements in security, efficiency, and customer confidence.

1. REDUCED COMPLIANCE COSTS

- **Automated Inventory & Access Control:** Eliminates the need for manual device tracking and user access reviews.
- **Audit-Ready Reporting:** Generates real-time compliance evidence, reducing audit preparation time and external consulting costs.
- **Lower Risk of Penalties:** Ensures continuous compliance, reducing the likelihood of fines for non-adherence.

Outcome: Compliance efforts are faster, more reliable, and less resource intensive.

2. IMPROVED RISK MANAGEMENT

- **Real-Time Visibility:** Detects and profiles every device, including BYOD, IoT, and rogue endpoints.
- **Faster Containment:** Identifies and quarantines non-compliant or infected devices in under **5 seconds**, limiting spread.
- **Proactive Security Posture:** Integrates with AV, XDR, SIEM, and firewalls to enforce Zero Trust across the enterprise.

Outcome: Stronger cyber resilience with reduced mean time to detect (MTTD) and respond (MTTR).

3. OPERATIONAL EFFICIENCY

- **Streamlined Governance:** Centralized management and reporting across multiple branches with the Central Visibility Manager (CVM).
- **Automated Response Workflows:** Security alerts from third-party tools trigger immediate NAC enforcement—no manual intervention.
- **Flexible Deployment:** No network redesign required, enabling faster rollout even at remote sites.

Outcome: Security operations run faster, smoother, and with fewer demands on IT staff.

4. ENHANCED CUSTOMER & REGULATOR TRUST

- **Transparent Compliance:** Demonstrates continuous adherence to BSP standards through clear reporting and audit trails.
- **Market Reputation:** Positions the institution as a security leader, strengthening customer loyalty.
- **Regulatory Confidence:** Builds trust with BSP examiners by aligning security practices with mandated frameworks.

Outcome: Greater confidence from customers, partners, and regulators, creating a competitive advantage.

In short, EasyNAC doesn't just help BSFIs check the compliance box—it lowers costs, reduces risk, improves efficiency, and builds the trust essential for long-term growth.

Conclusion

BSP-supervised financial institutions (BSFIs) face the dual challenge of meeting strict regulatory mandates under Circular 982 while defending against increasingly sophisticated cyber threats. The pressure to comply, protect sensitive financial data, and maintain operational resilience has never been greater.

EasyNAC addresses these challenges with a **network-agnostic, agentless platform** that simplifies compliance and strengthens security without adding network complexity. By combining continuous visibility, automated access control, and rapid incident containment, EasyNAC ensures BSFIs can:

- **Prove Compliance:** Demonstrate adherence to BSP 982 and related mandates with audit-ready reporting and automated policy enforcement.
- **Prevent Breaches:** Detect and quarantine unauthorized or compromised devices in seconds, stopping threats before they spread.
- **Protect Trust:** Safeguard the confidentiality, integrity, and availability of critical financial systems, building regulator and customer confidence.

With EasyNAC, compliance becomes more than a regulatory requirement—it becomes a foundation for stronger security, improved efficiency, and sustainable trust in the digital financial ecosystem.

End of Document