BRICS 2024
RUSSIA

BEST PRACTICES IN CONDUCTING PENETRATION TESTING AND VULNERABILITY ASSESSMENTS OF INFORMATION INFRASTRUCTURE FACILITIES

CONTENTS

Disclaimer

The designations employed and the presentation of the material in this publication do not imply expression of any opinion whatsoever on the part of the BRICS Central (Reserve) Banks concerning the legal status of any country, territory, city, area or its authorities, or concerning the delimitation of its frontiers or boundaries. The mention of specific companies or certain manufacturers' products does not imply that they are endorsed or recommended by the BRICS Central (Reserve) Banks in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters. All reasonable precautions have been taken by the BRICS Central (Reserve) Banks to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. The opinions, findings and conclusions expressed in this publication do not necessarily reflect the views of the BRICS Central (Reserve) Banks.

These best practices have been developed to establish a unified approach that financial institutions, whose activities fall under the purview of the BRICS Central (Reserve) Banks, could consider when conducting penetration testing and vulnerability assessments with regard to the information security of automated systems, software, hardware, and telecommunications equipment (hereinafter jointly referred to as "information infrastructure facilities").

1. BEST PRACTICES IN CONDUCTING PENETRATION TESTING AND VULNERABILITY ASSESSMENTS OF INFORMATION SECURITY

Best practices in this area include the following:

1.1. Determining the scope of penetration testing and vulnerability assessments:

- Define the critical assets, systems, and data to be included in the testing scope, ensuring alignment with business objectives and risk tolerance;
- Set clear boundaries to prevent disruptions to business operations and avoid unintentional impacts on production environments;
- Have a clear view of the attack surface to probe, enter, attack or maintain a presence in the system;
- Prioritise high-risk areas, such as systems with external exposure or those involved in critical financial transaction processing;
- Define assets to be tested (critical systems, data, applications).

1.2. Conducting penetration testing and vulnerability assessments with regard to automated systems, software, hardware, telecommunications equipment, and software that is distributed among clients to enable them to perform banking or financial transactions and is designed to process protected information at sites used for accepting electronic messages to be executed in automated systems and Internet-based applications, including:

- Online banking web applications;
- “Personal account” web applications for clients of financial organizations;
- Online banking mobile applications;
- Specialized online banking client applications (available on multiple operating systems);
- Automated systems enabling individuals and legal entities to use online banking services, including integration systems and APIs;
- Application servers and servers of database management systems;
- Any other critical systems (crown jewels).

Additional considerations include:

- Include both black-box (no prior knowledge) and white-box (full knowledge) testing to uncover external and internal vulnerabilities;
- Test for emerging threats (e.g., API security vulnerabilities, cloud infrastructure) and leverage both manual and automated tools;

- Consider social engineering techniques to assess the risk of human vulnerabilities, such as phishing.

1.3. Reporting the results of penetration testing and vulnerability assessments to the head of the organization/to leadership:

- Provide detailed technical reports, as well as high-level executive summaries, so that both technical staff and leadership can understand the findings;
- Include a clear prioritisation of vulnerabilities, recommended remediation actions, and timelines for addressing critical issues;
- Ensure accountability by assigning specific teams or individuals to carry out remediation efforts.

1.4. Registering Security and Operational Resilience Incidents:

- Develop processes for registering information security incidents related to penetration testing, categorising them by severity and impact;
- Conduct root cause analysis for each incident, documenting lessons learned to prevent future occurrences;
- Ensure incident registration is integrated into a centralised incident management system for efficient tracking and follow-up.

1.5. Reporting to Regulators:

- Follow mandatory compliance reporting guidelines for data breaches or for payment card systems;
- Report all detected vulnerabilities and security incidents to relevant regulators, detailing the causes, impact, and corrective actions taken;
- Maintain auditable records of all incidents, including near misses and potential vulnerabilities, to ensure transparency and accountability;
- Ensure timely reporting within required timeframes.

2. BEST PRACTICES IN CONDUCTING PENETRATION TESTING OF INFORMATION INFRASTRUCTURE FACILITIES

2.1. Conducting External and Internal Penetration Testing:

- **External Penetration Testing:** Focus on external-facing systems such as web applications, VPNs, cloud infrastructure, and other internet-exposed assets to simulate an external attacker's actions;
- **Internal Penetration Testing:** Simulate insider threats or compromised employee accounts, testing for privilege escalation and lateral movement across internal networks. Pay special attention to areas where least-privilege principles should be applied.

2.2. Using the following methods when conducting penetration testing:

- Black-box testing, whereby the tester does not possess any information on information infrastructure facilities at the financial market organization;
- Grey-box testing, whereby the tester possesses partial information on information infrastructure facilities at the financial market organization;
- White-box testing, whereby the tester possesses complete information on information infrastructure facilities at the financial market organization.

2.3. Leveraging Threat Databases and Intelligence Feeds:

- Using databases of information security threats and other information sources for the purposes of identifying vulnerabilities and presenting results in a formalized manner (for instance, CAPEC,[1] MITRE ATT&CK,[2] OWASP,[3] STIX,[4] WASC,[5] CWE,[6] CVE,[7] and others) when conducting penetration testing;
- Tailor the penetration testing approach based on threat models relevant to the financial sector, focusing on common attack techniques (e.g., those used by advanced persistent threats targeting financial institutions);
- Combine real-time threat intelligence feeds with traditional vulnerability databases to stay informed of emerging threats and risks.

[1] Common Attack Pattern Enumeration and Classification, accessible at https://capec.mitre.org.

[2] MITRE ATT&CK, accessible at https://attack.mitre.org.

[3] Open Web Application Security Project, accessible at https://owasp.org.

[4] Structured Threat Information Expression, accessible at https://stixproject.github.io.

[5] Web Application Security Consortium, accessible at https://www.webappsec.org.

[6] Common Weakness Enumeration, accessible at https://cwe.mitre.org.

[7] Common Vulnerabilities and Exposures, accessible at https://cve.mitre.org.

2.4. Taking into account the potential of the perpetrator indicated in the information security threat model when conducting penetration testing. Moreover, it is good practice to use automated tools that help simulate attacks accounting for the identified vulnerabilities.

2.5. Customise the threat model based on the organisation's risk profile, considering the potential actions of relevant threat actors, such as cybercriminals or insider threats.

2.6. Use automated attack simulation tools to simulate multi-vector attacks and account for identified vulnerabilities. Complement automated tools with manual testing to identify business logic flaws and complex attack scenarios.

2.7. Complementing the results of penetration testing with a comparison between the obtained results and the anticipated results (which were indicated in the terms of reference for the penetration testing and vulnerability assessment).

2.8. Recording the actual results of penetration testing and studying the causes of any unforeseen situations:

- Record all penetration testing results, paying particular attention to any unforeseen situations that arise during testing;
- Conduct a post-mortem analysis of unexpected issues, documenting both technical and procedural causes to enhance future security efforts;
- Store all testing results and analysis in a centralised system (e.g., a SIEM) to correlate with other security incidents and improve the overall security posture.

2.9. Conducting another round of penetration testing after the identified vulnerabilities have been eliminated. Re-Testing Vulnerabilities:

- After vulnerabilities have been remediated, conduct another round of penetration testing to verify that the fixes were successfully implemented and no new vulnerabilities were introduced;
- Expand the scope of re-testing where necessary to ensure comprehensive coverage of any new security risks that may have emerged during the remediation process.

2.10. Penetration testing may be conducted by appropriately trained and independent information security experts/auditors.

2.11. In the post implementation (of IT project/system upgrade, etc.) scenario, the penetration testing may be performed on the production environment. Under unavoidable circumstances, if the penetration testing is conducted in test environment, organizations may ensure that the version and configuration of the test environment resembles the production environment.

3. BEST PRACTICES IN CONDUCTING VULNERABILITY ASSESSMENTS OF INFORMATION SECURITY

3.1. Scanning for Vulnerabilities:

- Perform systematic vulnerability scanning for code errors in software, including system-wide, application-specific, and specialised software. Ensure that this includes software used for information protection tools, hardware devices, and other technical components;
- Prioritise software and systems handling sensitive financial data or those providing access to critical financial operations.

3.2. Identification, Assessment and Elimination of Vulnerabilities:

- Conducting identification, assessment of vulnerabilities throughout the entire lifecycle of the organisation's information infrastructure, from development to operational stages;
- Ensure that vulnerability assessment is a continuous process, conducted regularly and when significant changes to the infrastructure occur;
- Implement a structured remediation plan that includes prioritisation based on risk and impact, and verify that eliminated vulnerabilities do not re-emerge during operations.

3.3. Organisations shall ensure to fix the identified vulnerabilities and associated risks in a timebound manner by undertaking requisite corrective measures and ensure that the compliance is sustained to avoid recurrence of known vulnerabilities such as those available in Common Vulnerabilities and Exposures (CVE) database.

3.4. These practices should be continuously implemented in the secure software development process of financial institutions.

4. BEST PRACTICES IN CONDUCTING PENETRATION TESTING AND VULNERABILITY ASSESSMENTS THROUGH A THIRD-PARTY SERVICE PROVIDER

4.1. Engaging a third-party service provider for the purpose of conducting penetration testing and vulnerability assessments, provided that it meets the following requirements:

- The provider has obtained a licence for performing the relevant type of activities, other applicable permits or approval of the national regulator;
- The provider has at least three years of experience in conducting penetration testing at financial market organizations confirmed by three or more completed agreements (contracts);
- The provider must ensure that all experts involved in testing have at least three years of verified experience in penetration testing;
- Providers should also demonstrate adherence to relevant industry standards/guidelines for security assessments;
- Non-Disclosure Agreement should be signed by the provider prior to commencing the penetration testing;
- Setting up of a well-defined mechanism to ensure secure handling of report and data at transit and rest;
- Penal provisions shall be included by the organisation into third-party contractual arrangements for any non-compliance by the application provider.

4.2. Granting authorisation to participate in penetration testing only to those experts of a third-party service provider who have not been engaged in developing requirements for the information infrastructure facilities' protection systems, or in designing, introducing and evaluating the conformity of the information infrastructure facilities' protection systems. This ensures unbiased results and eliminates conflicts of interest in the assessment process.

5. BEST PRACTICES IN CONDUCTING UNASSISTED PENETRATION TESTING AND VULNERABILITY ASSESSMENTS OF INFORMATION INFRASTRUCTURE FACILITIES

5.1. Conducting penetration testing and vulnerability assessments without assistance in the following cases:

- In case of changes being made to the architecture and/or configuration of information infrastructure facilities without affecting the operations of critical information infrastructure objects or functions related to ensuring information security;
- In case of verifying the elimination of vulnerabilities identified during penetration testing conducted with assistance of a third-party service provider;
- Other scenarios as deemed appropriate by the regulator, considering specific organisational risk profiles.

5.2. Designating Internal Units of Experts:

- Establish a dedicated internal team or unit responsible for penetration testing and vulnerability assessments, ensuring the team has sufficient expertise and resources;
- Designate staff members who are not involved in the day-to-day information security management of the infrastructure to avoid conflicts of interest.

5.3. Assigning Information Security Responsibilities:

- Ensure that the personnel responsible for the security of the information infrastructure are distinct from those conducting the penetration testing. This separation of duties helps maintain objectivity and reduces the risk of internal bias.

5.4. Appoint of Qualified Experts:

- Appoint at least two experts with at least three years of experience in penetration testing and vulnerability assessments to conduct the assessments;
- Ensure that these experts receive annual advanced training in penetration testing and vulnerability assessment to stay updated on the latest techniques and threats.

5.5. Not allowing the engagement of concerned officials (developers, owners, administrators and information security administrators of the information infrastructure facilities that will be subject to the penetration testing and vulnerability assessment) in any activities related to penetration testing and vulnerability assessments of information infrastructure facilities. This helps maintain the integrity and objectivity of the testing process.

5.6. Organisations shall ensure that all vulnerability scanning is performed in authenticated mode either with agents running locally on the system to analyse the security configuration or with remote scanners that are given administrative rights on the system being tested.

6. BEST PRACTICES IN DOCUMENTING PENETRATION TESTING AND VULNERABILITY ASSESSMENTS OF INFORMATION SECURITY

6.1. Organisations to put in place a documented approach for conduct of vulnerability assessments / penetration testing covering the scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System) and all other aspects. This may also apply to the information systems hosted in a cloud environment. Prior to conducting penetration testing and a vulnerability assessment, for the purpose of implementing measures aimed at minimizing the negative consequences of information infrastructure facilities' information security being compromised during such testing, financial market organizations are advised to:

6.1.1. Develop and/or update the following documents:

- Terms of reference (TOR) for the penetration testing and vulnerability assessment , which includes clear objectives, scope, and methodologies;
- Agreement on the liability of the parties to and participants in the penetration testing and vulnerability assessment;
- Threat models tailored to the organisation's information infrastructure, outlining potential attack vectors and risks;
- Operational resilience recovery plans to address emergency situations that may arise during testing.

6.1.2. Indicate the following information in their TORs:

- A detailed list of services;
- The number of stages of testing;
- Timeline for the provision of services;
- Objectives of the services provided;
- List of regulations under which the services are provided;
- Operational resilience recovery plans to address emergency situations that may arise during testing;
- A list of infrastructure components that are excluded from the testing perimeter, along with the reasons for their exclusion (e.g., bandwidth or time constraints);
- Method (procedure) for conducting the penetration testing and vulnerability assessment, including:
    - Types of potential attacks (attack surfaces, as well as techniques and tactics) and vulnerabilities to be simulated;
    - The tools and techniques to be used in the penetration testing and vulnerability assessment;

- The environment in which the testing will occur (e.g., a test environment that mirrors the production environment);
- Network diagrams detailing the addresses and subnetworks included in the testing scope;
- A list of activities that are restricted during testing, such as targeting employees' private devices or using coercive tactics;
- Conditions that will trigger the immediate termination of testing;
- Expected outcomes, including criteria for assessing whether the testing is complete or if further testing is needed;
- Templates for the reporting of findings;
- Timeframes and conditions for any repeat testing;
- List of databases of information security threats, and other information sources used for identifying vulnerabilities.

6.1.3. Furthermore, when conducting penetration testing and vulnerability assessments, it is recommended to use Supporting Documentation.
During penetration testing, organisations should follow the provisions of the following documents:

- Agreement authorizing the testing of critical addresses and subnetworks;
- Agreement on non-disclosure of confidential information;
- Documentation on information protection tools, including their configurations and applied settings;
- Rules of allocating accounts for experts engaged in penetration testing (if necessary);
- Password policies implemented at information infrastructure facilities;
- User manuals for information infrastructure facilities;
- Administrator manuals for information infrastructure facilities;
- Work schedule of the financial market organization's employees to ensure testing is conducted without operational disruptions.

6.1.4. The following is advised with regard to the results of penetration testing and a vulnerability assessment:

- Reporting and preservation of Results: The results or penetration testing and vulnerability assessments should be documented in a report either in paper or electronic format: The recommended format of such report is presented in the Annex to this document;
- Paper reports should be sealed to prevent tampering;
- Electronic reports should be provided in a non-editable format, such as one signed with an electronic signature;
- It is recommended that reports be preserved for at least five years or based on jurisdictional requirements to maintain a historical record and to ensure regulatory compliance.

ANNEX. RECOMMENDED FORMAT OF A PENETRATION TESTING AND VULNERABILITY ASSESSMENT REPORT

Report on the results of the penetration testing and vulnerability assessment of information infrastructure facilities' information security at

<name of the financial market organization>

1. General provisions:

- Description of the assessed facilities;
- Overview of the conducted testing;
- Brief description of the results of the penetration testing and vulnerability assessment of the information infrastructure facilities' information security;
- Period when the penetration testing was conducted;
- Full names and positions of the experts conducting the penetration testing;
- Information on the accounts and roles assigned for conducting the penetration testing (if any);
- Additional information provided for the purpose of penetration testing;
- Description of the potential of the perpetrator compromising information security, compiled in accordance with the model of threats to information security;
- Description of the negative consequences and/or unacceptable events that can occur in case the vulnerabilities are exploited;
- List of access facilities with regard to which unauthorised access may be gained by using the vulnerabilities identified;
- List of penetration testing types, indicating the facilities tested;
- Description of the penetration testing's exclusion scope indicating the reasons for these exclusions or information on the absence of such exclusions.

2. Penetration testing methodology:

- Description of the penetration testing stages;
- Description of the conditions and consolidated results of the penetration testing.

3. Description of the identified vulnerabilities:

- Comprehensive list of the identified vulnerabilities;
- Tools used in the course of the penetration testing;
- IP address of the scanned facility, its DNS name (if any), and any other information that would enable unambiguous identification of the information system or its part being analysed.

4. Vulnerability exploitation:

- Description of how the attack models were applied, including the models' algorithms, that demonstrates the possibility of exploiting the identified vulnerabilities;
- Date and time when the attack models were applied;
- Description of the negative consequences and/or unacceptable events that can occur in case the identified vulnerabilities are exploited.

5. Recommendations for elimination:

- Description of vulnerabilities, indicating their criticality;
- Recommendations for eliminating vulnerabilities.

BRICS RAPID INFORMATION SECURITY CHANNEL (BRISC) MEMBERS

Members	Position, Organisation
Central Bank of the Russian Federation (as the chair)	
Mr. Maxim Leonov	BRICS Coordinator, Consultant, Department for Cooperation with International Organizations
Ms. Evgeniya Molotova	BRICS Coordinator, Chief Economist, Department for Cooperation with International Organizations
Mr. Kirill Shumei	BRICS Coordinator, Lead Economist, Department for Cooperation with International Organizations
Mr. Andrey Vybornov	Deputy Director, Information Security Department, Ph.D. in Technology
Mr. Grigory Tsarev	Deputy Head of the Financial CERT
Mr. Alexander Chuburkov	Consultant, Information Security Department
Mr. Alexei Kudrin	Chief Engineer, Information Security Department
South African Reserve Bank	
Ms. Samantha Springfield	Head, IERPD
Ms. Philadelphia Makhanya	Manager, IERPD
Mr. Gerhard Cronjé	Divisional Head, Cyber and Information Security, Business Systems and Technology Department
Ms. Yolande Poley	BRICS Coordinator, International Economic Relations and Policy Department (IERPD)
Ms. Motshidisi Mokoena	Senior Economic Policy Analyst, IERPD
Mr. Jacques Théron	Financial Sector Cyber Security Consultant, Business Solutions and Technology Department
Central Bank of the United Arab Emirates	
Mr. Thabet Bakheet Khamis	Chief Risk Officer
Mr. Hamed Obaid Areidat	Senior Director – IT Operations
Mr. Bader Ali Murad Mohammed	Team Lead – Information Security
Central Bank of Brazil	
Mr. Haroldo Jayme Martins Froes Cruz	Head of the Information Technology Department
Mr. Aristides Andrade Cavalcante Neto	Head of the Strategic Management and Specialized Supervision Department
Mr. Marcelo Antonio Thomaz de Aragão	Head of the International Affairs Department
Ms. Veruska Rocha de Aragão	Deputy Head of the Information Technology Department
Mr. Marcelo Colli Inglez	Deputy Head of the Strategic Management and Specialized Supervision Department
Ms. Bianca Viana Cardoso Kivel	Deputy Head of the International Affairs Department

Members	Position, Organisation
People's Bank of China	
Mr. Shen Xiaoyan	Division Chief, Technology Department
Mr. Wang Tao	Level IV Division Rank Official, Technology Department
Mr. Tan Leiyu	Staff, Technology Department
Mr. Dai Chen	Staff, Technology Division, PBOC Jiangsu Branch
Central Bank of Egypt	
Dr. Sherif Hazem	CBE Sub-Governor and Cyber Security Sector Head
Dr. Ibrahim Mostafa	CBE Assistant Sub-Governor and EG-FinCIRT Director
Eng. Karim Wahba	Cyber Intelligence and Vulnerability Handling Head – EG-FinCIRT
Eng. Mahmoud Abdelbary	R&D Team Leader – EG-FinCIRT
Eng. Sherif Embaby	Cyber Intelligence Team Leader – EG-FinCIRT
National Bank of Ethiopia	
Mr. Windewosen Tsegaw Feleke	Director, Information System Management Directorate, National Bank of Ethiopia
Reserve Bank of India	
Dr. Sanjay Bahl	Director General, CERT-In
Mr. T. K. Rajan	Chief General Manager-in-Charge, Department of Supervision, RBI
Mr. Noorul Ameen	Scientist 'E', CERT-In
Mr Vinod Kumar Chouhan	Scientist, Ministry of Electronics & Information Technology
Ms. Darshana S Kulkarni	General Manager, Department of Information Technology, Reserve Bank of India
Mr. Sreejith S	Assistant Manager, International Department, RBI
Central Bank of the Islamic Republic of Iran	
Mr. Najmeh Ramouz	Head of Group, International Strategic Cooperation, Central Bank of the Islamic Republic of Iran

BRICS RAPID INFORMATION SECURITY CHANNEL (BRISC) EDITORIAL TEAM

Members	Position, Organisation
Central Bank of the Russian Federation (as the chair)	
Mr. Alexander Chuburkov	Editor-in-Chief, Consultant, Information Security Department, GOST R expert
Mr. Konstantin Starodubov	Co-Editor, Consultant, Information Security Department, Ph.D. in Technology
Mr. Ilya Gushcha	Contributor, Lead Engineer, Information Security Department
Mr. Igor Litvinov	Contributor, Chief Engineer, Information Security Department
Mr. Viktor Kuchin	Linguistic Support, Head of Unit, Department for Cooperation with International Organizations
Mr. Mikhail Godunov	Linguistic Support, Consultant, Department for Cooperation with International Organizations
Ms. Lidia Yarina	Linguistic Support, Consultant, Department for Cooperation with International Organizations
Ms. Alexandra Marsova	Linguistic Support, Lead Expert, Department for Cooperation with International Organizations
Ms. Tatiana Shevlyakova	Linguistic Support, 1st cat. Expert, Department for Cooperation with International Organizations
South African Reserve Bank	
Mr. Gerhard Cronjé	Head of Cyber and Information Security Unit
Mr. Jacques Théron	Financial Sector Cybersecurity Consultant
Central Bank of the United Arab Emirates	
Mr. Thabet Bakheet Khamis	Chief Risk Officer
Central Bank of Brazil	
Mr. Alexander Bulbow	Coordinator, Strategic Management and Specialized Supervision Department
Mr. Estenio do Nascimento Cabral	Advisor, Information Technology Department
People's Bank of China	
Mr. Shen Xiaoyan	Division Chief, Technology Department
Mr. Wang Tao	Level IV Division Rank Official, Technology Department
Mr. Tan Leiyu	Staff, Technology Department
Mr. Dai Chen	Staff, Technology Division, PBOC Jiangsu Branch
Central Bank of Egypt	
Eng. Mostafa Hesham	Cyber Security Governance and Assessment – Cyber Security Sector
Eng. Ahmed Anas	Cyber Security Governance – Cyber Security Sector
National Bank of Ethiopia	
Mr. Windewosen Tsegaw Feleke	Director, Information System Management Directorate, National Bank of Ethiopia
CERT-In and Reserve Bank of India	
Mr. Pradeep Raj Singh	General Manager, Department of Supervision, RBI
Mr. Ashutosh Bahuguna	Scientist 'E', CERT-In
Mr. Devender Yadav	Officer on Special Duty, CSIRT-Fin, CERT-In
Mr. Shashank Gupta	Scientist 'C', CERT-In
Mr. Saikrishna Medishetti	Manager, Department of Supervision, RBI
Central Bank of the Islamic Republic of Iran	
Mr. Najmeh Ramouz	Head of Group, International Strategic Cooperation, Central Bank of the Islamic Republic of Iran