Enhancing Cyber Security Measures in NADRA and Folio3: Safeguarding National Identity Data

Professional Practices in IT - PPIT

Team

Abdul Ahad Shaikh (20K-0319)

Muhammad Basil Ali Khan (20K-0477)

Syed Ali Jodat (20K-0155)

Course Teacher

Sir Shoaib Rauf

Company and Interview - 1

Company - NADRA

Conversation with:

Ahmerin Hussain (Security Head Sharah-e-Quaideen Branch)

About NADRA

- NADRA, established in 2000, was formed to modernize Pakistan's identity management system, ensuring efficient citizen registration and authentication services nationwide. It played a pivotal role in digitizing identity documentation, streamlining processes, and establishing a centralized database for identity-related services in Pakistan

Company and Interview - 2

Company – Folio3

Conversation with:

Muhammad Saeed (Information Security Specialist)

About Folio3

- Folio3 is a software development company known for its expertise in crafting innovative digital solutions across various industries. Specializing in software development, mobile apps, AI, IoT, and cloud services, Folio3 has a reputation for creating cutting-edge software tailored to clients' needs.

TABLE OF CONTENTS

01 NADRA'S APPROACH TO CYBER-SECURITY

02 NADRA'S CYBER-SECURITY MEASURES AND PROTOCOLS

03 NADRA'S INCIDENT RESPONSE AND RECOVERY

04 NADRA'S INCIDENT RESPONSE AND RECOVERY

05 NADRA'S DATA PRIVACY AND COMPLIANCE

06 NADRA'S SECURITY INFRASTRUCTURE AND TECHNOLOGY

07 NADRA'S RISK MANAGEMENT AND ASSESSMENT

08 NADRA'S COMPLIACE WITH INDUSTRY STANDARDS

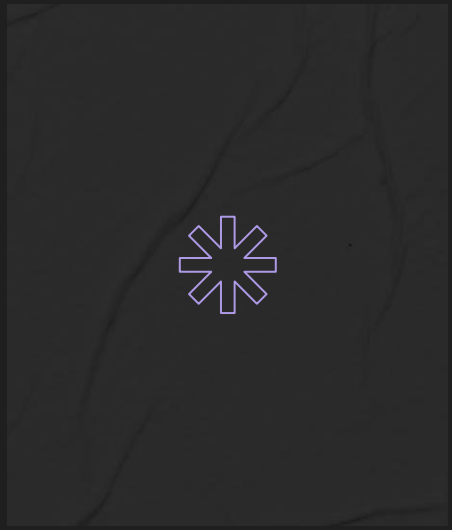
09 NADRA'S COLLABORATION AND REPORTING

10 NADRA'S INCIDENT RESPONSE EVALUATION

11 CONCLUSION

01

NADRA AND FOLIO3'S APPROACH TO CYBER-SECURITY



NADRA AND FOLIO3'S APPROACH TO CYBER-SECURITY

NADRA

- NADRA adopts a risk-based approach, focusing on identifying and mitigating potential threats through continuous risk assessments.
- This means that they solve the issue whenever the problem occurs, rather than taking measures before the issues take place.
- This might be problematic as NADRA might solve the issue after the data leak occurs which causes a breach in National Data Security.

FOLIO3

- FOLIO follows a proactive security approach, implementing robust measures to prevent potential cyber threats before they occur.
- This means that they try to solve the issue before the problem occurs, which helps from preventing hackers from doing anything in the first place.
- This is a plus point, however, if there are new threats which they have not solved yet, then it is very problematic and rigorous to prevent that, as they have to work on that from scratch.

NADRA's adaptable approach suits evolving threats, while FOLIO's proactive stance might be advantageous for preventing potential risks

“I dream a digital Pakistan, where Cyber Security becomes an Integral Part of our National Security”

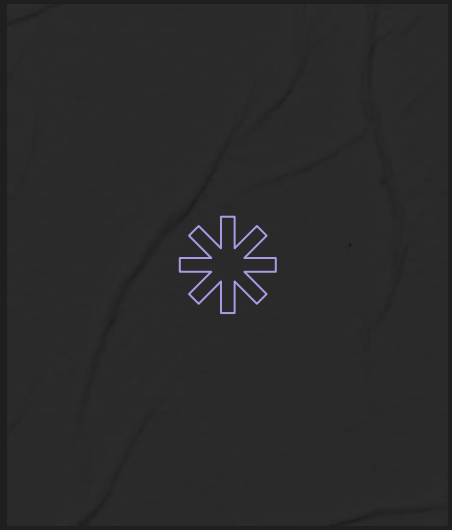
-Ahmerin Hussain

231,400,000

Population of Pakistan – All need to protect their Data

02

NADRA'S AND FOLIO3'S CYBER-SECURITY MEASURES AND PROTOCOLS



NADRA AND FOLIO3'S CYBER-SECURITY MEASURES AND PROTOCOLS

NADRA

- NADRA employs encryption, access controls, and regular security patches to safeguard data.
- NADRA encrypts sensitive data. This makes the data unreadable even if it is hacked.
- It also involves strict access controls where only people with authorization can see the data.
- NADRA does regular security patches, which means it constantly updates its software to prevent and kind of new cyber security threat.

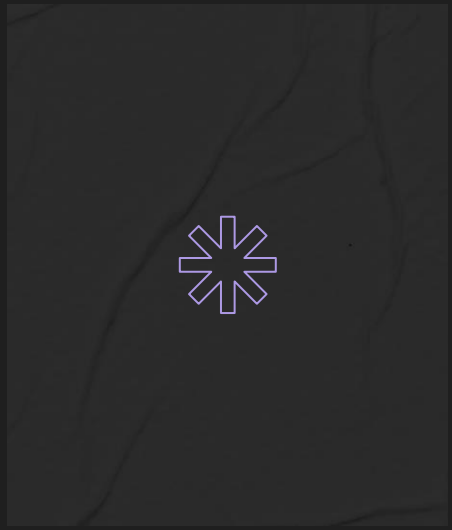
FOLIO3

- FOLIO prioritizes network segmentation, penetration testing, and intrusion prevention systems.
- FOLIO uses network segmentation, dividing its network into different parts, this limits the impact of cyber attack by preventing lateral movement across the network.
- Regular penetration testing to identify potential vulnerabilities within systems. This is so that threats can be prevented before they even occur.
- FOLIO uses IPS which actively monitors traffic for suspicious activity as well.

Determining the "better" approach depends on the specific threats faced, with NADRA prioritizing data protection measures and FOLIO focusing on network fortification.

03

NADRA AND FOLIO'S INCIDENT RESPONSE AND RECOVERY



NADRA AND FOLIO'S INCIDENT RESPONSE AND RECOVERY

NADRA

- NADRA might have a well-defined incident response plan, with clear roles and procedures for handling security breaches.
- NADRA likely has a structured incident response plan, detailing specific roles, responsibilities, and procedures for handling security breaches. This plan is likely comprehensive and documented, outlining steps to detect, contain, and mitigate security incidents.

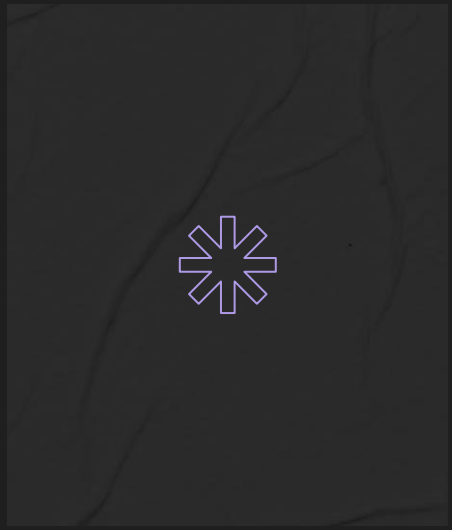
FOLIO3

- FOLIO could emphasize quick detection, swift containment, and efficient recovery protocols following a security incident.
- Quick Identification: Rapidly identifies any potential security threats if they occur.
- Swift Containment: Upon detection, FOLIO immediately contains the spread or impact.
- Efficient recovery: Efficiently focuses on recovery protocols, involving restoring effected system.

NADRA's defined plan may be better for structured handling, while FOLIO's swift response might minimize operational downtime more effectively.

04

NADRA’S AND FOLIO’S EMPLOYEE TRAINING AND AWARENESS



NADRA'S AND FOLIO'S EMPLOYEE TRAINING AND AWARENESS

NADRA

- NADRA may conduct regular cybersecurity training for employees, including simulated phishing exercises and awareness campaigns.
- Stimulated phishing exercises: Sending mock phishing emails to employees to test their awareness and ability to recognize and report suspicious emails.
- Awareness Campaigns: Runs awareness campaigns to educate employees importance of cyber security.

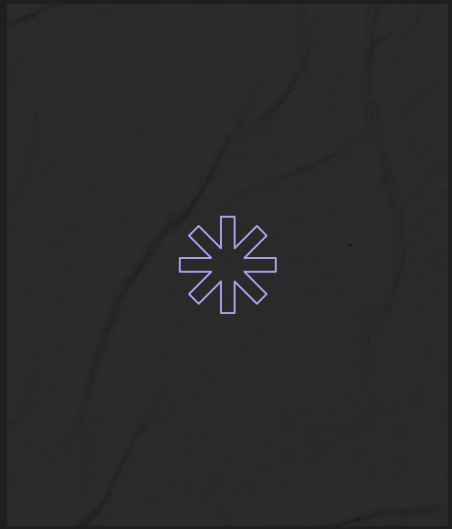
FOLIO3

- FOLIO might focus on creating a security-conscious culture, ensuring employees are informed and vigilant about potential threats.
- Security Conscious Culture: Mindset that every employee understands their roles in maintaining cyber-security.
- Continuous Information: Ensuring that every employee is updated with the latest threats.

Both have strengths; NADRA's training initiatives and FOLIO's cultural focus can complement each other based on organizational culture.

05

NADRA AND FOLIO'S DATA PRIVACY AND COMPLIANCE



NADRA AND FOLIO'S DATA PRIVACY AND COMPLIANCE

NADRA

- NADRA prioritizes compliance with data protection laws, implementing stringent data handling and privacy policies.
- Stringent Data handling policies: Defines clear guidelines on data access, encryption, and disposal to maintain data integrity and confidentiality.
- Privacy policies: Comprehensive privacy policies to inform individuals about how their data is collected, used and protected.

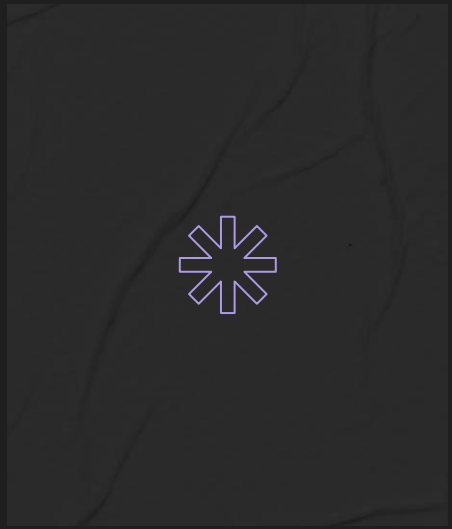
FOLIO3

- FOLIO focuses on ensuring adherence to global privacy regulations like GDPR and CCPA, implementing privacy-enhancing technologies.
- Data governance and Compliance Measures: Folio might have stringent government measures in place, including regular audits, assessments and documentation to ensure ongoing compliance with global privacy regulations.

NADRA's continuous assessment adapts well to evolving threats, whereas FOLIO's proactive strategies may mitigate risks before they manifest.

06

NADRA AND FOLIO'S SECURITY INFRASTRUCTURE AND TECHNOLOGY



NADRA AND FOLIO'S SECURITY INFRASTRUCTURE AND TECHNOLOGY

NADRA

- NADRA invests in cutting-edge intrusion detection systems and adaptive security architectures.
- Advanced intrusion detection systems: These system continuously monitor network traffic and systems for suspicious activities or potential security breaches.
- Adaptive Security architectures: These architectures are designed to dynamically adjust security measures based on the evolving threat landscape.

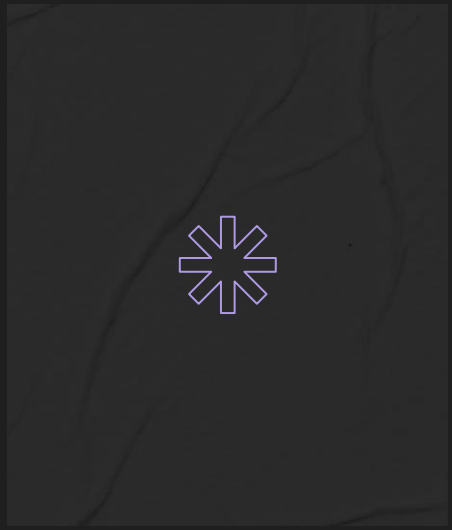
FOLIO3

- FOLIO might prioritize secure coding practices and regular technology updates.
- Secure Coding practices: Minimizes vulnerabilities and weaknesses in the code that could be exploited by hackers.
- Regular technological updates: FOLIO prioritizes systems and software up to date with the latest security patches, updates and fixes.

NADRA's adherence to local laws and FOLIO's compliance with global standards both have merits based on the organization's global reach and regulatory environment.

07

NADRA AND FOLIO'S RISK MANAGEMENT AND ASSESSMENT



NADRA AND FOLIO'S RISK MANAGEMENT AND ASSESSMENT

NADRA

- NADRA places emphasis on continuous risk assessments such as Iterative Risk Management to adapt security measures to evolving threats.
- Iterative risk assessment: This involves regularly evaluating the organization's systems, networks, and data to identify potential vulnerabilities and threats.

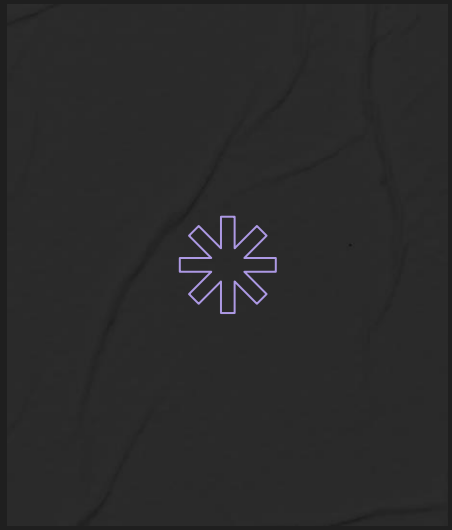
FOLIO3

- FOLIO Focuses on proactive risk management strategies, employing advanced technologies to mitigate potential risks preemptively.
- Proactive risk management: FOLIO focusses on employing advanced technologies to proactively mitigate potential risks before they materialize. This involves using predictive analysis, threat intelligence, and other advanced tools to anticipate and prevent security incidents.

Both have distinct strengths; NADRA's investments in cutting-edge systems and FOLIO's emphasis on secure coding complement different security aspects.

08

NADRA’S AND FOLIO’S COMPLIACE WITH INDUSTRY STANDARDS



NADRA'S AND FOLIO'S COMPLIACE WITH INDUSTRY STANDARDS

NADRA

- NADRA aligns with local and industry-specific standards, focusing on compliance with relevant regulations.
- Focus on relevant regulations: This includes adhering to local laws, industry up to date technologies, and standards by NADRA with their own operational jurisdiction.

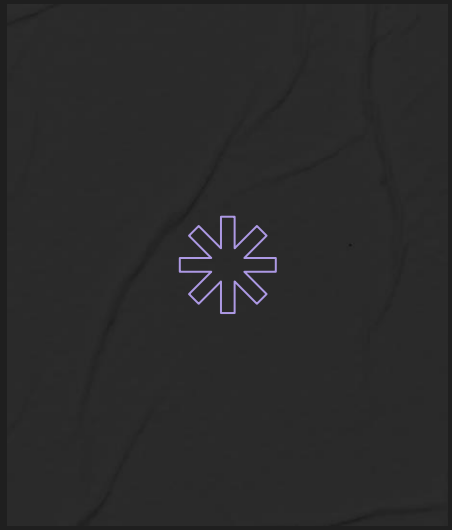
FOLIO3

- FOLIO ensures adherence to global standards like NIST Cybersecurity Framework, aiming for a broader spectrum of security coverage.
- NIST Framework: This framework provides a comprehensive set of guidelines, best practices, and standards applicable across various industries and geographical regions.
- FOLIO aims for more comprehensive security posture. It focuses on implementing measures and protocols that cover a wide range of potential threats and security domains.

Again, it depends on the organization's scope; NADRA's alignment with local standards and FOLIO's adherence to global ones can both be beneficial.

09

NADRA’S AND FOLIO’S COLLABORATION AND REPORTING



NADRA'S AND FOLIO'S COLLABORATION AND REPORTING

NADRA

- NADRA emphasizes cross-departmental collaboration for threat intelligence sharing and structured incident reporting.
- Cross departmental collaboration: Involves sharing potential cyber threats, vulnerabilities or incidents across the organization to enhance overall awareness.
- Structured incident reporting: This ensures when security incidents occur, there's a defined process for reporting, documenting and handling these incidents.

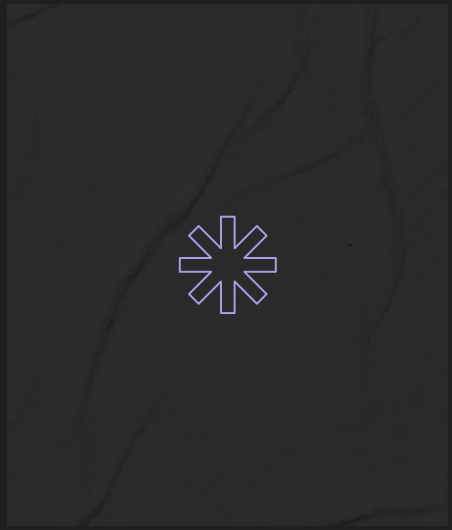
FOLIO3

- FOLIO ensures transparent reporting structures for incidents and updates across the organization to maintain visibility and accountability.
- Incident transparency: This means that ensuring that incidents, security updates, and relevant information are communicated openly across the organization.
- Visibility and accountability: FOLIO's approach aims to maintain visibility into security incidents and updates. This helps in keeping all stakeholders informed and accountable for their roles in cybersecurity

NADRA's cross-departmental collaboration and FOLIO's transparent reporting structures offer different advantages based on organizational culture and communication needs.

10

NADRA AND FOLIO'S INCIDENT RESPONSE EVALUATION



NADRA AND FOLIO'S INCIDENT RESPONSE EVALUATION

NADRA

- NADRA focusses on post-incident reviews to refine response strategies and improve future incident handling.
- Refine response strategies: This involves analyzing the response to security incidents in detail, identifying strengths, weaknesses and areas for improvement.
- Learning from past incidents: NADRA also focusses on learning from past incidents and not letting that happen ever again.

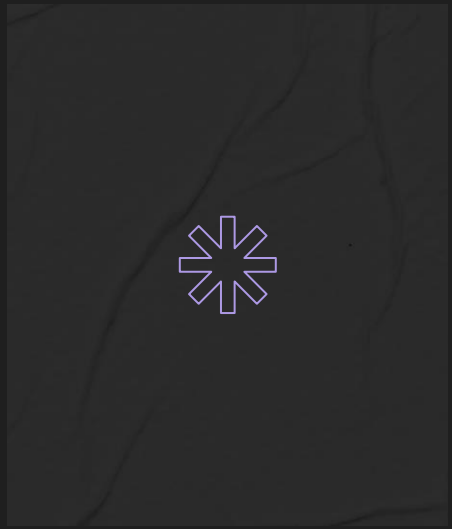
FOLIO3

- FOLIO prioritizes incident trend analysis and continuous improvement, ensuring lessons learned are integrated for ongoing enhancement.
- Incident Trend Analysis: Involves tracking patterns, or emerging threats observed across multiple incidents to identify commonalities and trends.
- Continuous Improvement: This means that gaining insights from analyzing incidents to continuously enhance and update incident response protocols.

NADRA's focus on post-incident reviews aids refinement, while FOLIO's trend analysis drives ongoing improvement.

11

Conclusion



CONCLUSION

If we look from Cyber Security’s POV, both NADRA and FOLIO exhibit strengths tailored to their unique needs. NADRA's adaptability to changing risks and structured incident response are commendable. Meanwhile, FOLIO's proactive risk management and transparent reporting foster continuous improvement. Deciding which is better depends on how well these strategies fit specific organizational needs, regulations, and their ability to tackle emerging threats. Both NADRA and FOLIO offer strong cybersecurity policies, highlighting the importance of diverse and adaptable approaches in defending against evolving cyber risks.

Interview with Mr. Ahmerin Hussain

THANKYOU