nodeZro
cyber intelligence solutions

Identity Impact Taxonomy for Digital Namespaces

A unique framework to strengthen identity management strategies.

THINK BEFORE YOU PRINT

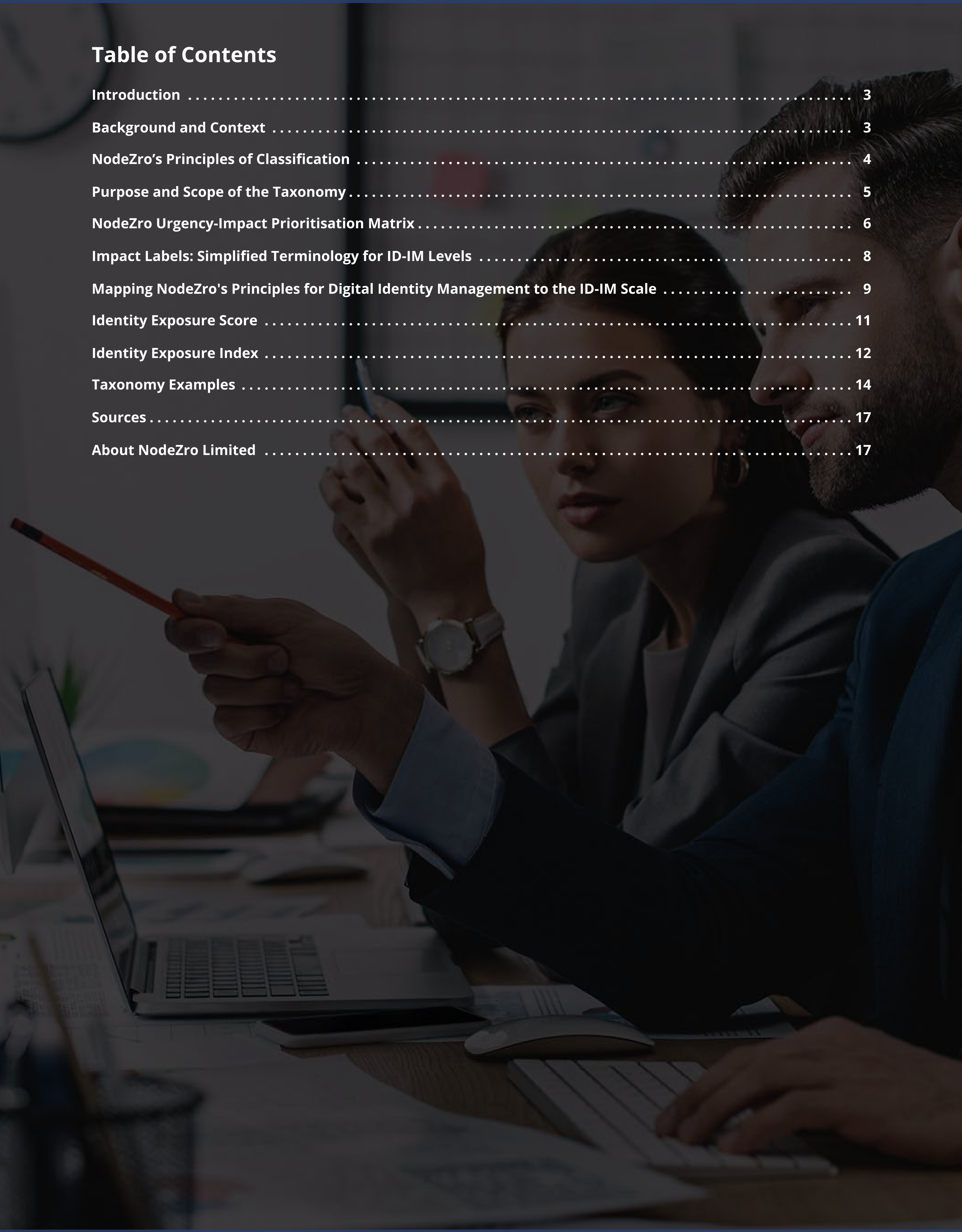


Table of Contents

Introduction

NodeZro’s Identity Impact Taxonomy is a unique framework designed to strengthen digital identity management strategies. This system organises workflows in a structured, methodical way, ranking various types of findings according to their potential impacts on an organisation.

Background and Context

As the wave of digital transformation intensifies, the importance of securing and managing digital identities for organisations is becoming increasingly critical. A digital identity namespace encompasses the online identifiers linked with an organisation, such as domain names and subdomains, email addresses and social media handles. These digital identifiers form not only the trust anchor of an organisation's brand and operations but also epitomise its online presence and serve as a communication point for employees, customers, and other stakeholders.

Despite their importance, digital namespace identities frequently succumb to management neglect, sporadic curation, poor lifecycle management, and security gaps. These oversights can generate a range of findings that could potentially damage an organisation's brand, trust and reputation as well as hinder its operations. Even a simple spelling error, affecting a single character in the configuration of a digital identity could precipitate a catastrophic breach. If these problems are left unresolved, they can pose a significant risk, potentially eroding the trust and credibility that stakeholders have in the organisation and its brand.

Moreover, the accelerated use of the Domain Name System (DNS) (7) in connecting an organisation's identity to third-party services, due to the shift towards Software as a Service (SaaS) (14) and cloud services, introduces additional challenges. These include the need for effective lifecycle management of digital identities, often represented as domains and subdomains.

Complicating matters further, the consolidation of legacy systems frequently results in a swath of identities being left unmanaged, as many organisations do not have established processes for handling the lifecycle management of their digital identities. Similarly, merger and acquisition activities can exponentially expand an organisation's identity space, often leading to a surge in unknown and unmanaged identities. Organisations sometimes acquire brands with a history of neglected identity lifecycle management, consequently exposing themselves to unmanaged post-acquisition risks.

> ***"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."***
>
> *Warren Buffet*

More worryingly, many of these findings can leave the organisation vulnerable to Corporate Identity Theft, a severe security breach involving the theft or misuse of the organisation's trusted identity. The consequences of such breaches can be disastrous, potentially inflicting significant short and long-term damage to the organisation, its reputation, and its stakeholders. Therefore, it is essential for organisations to pay due diligence to the management and security of their digital identities in this era of rapid digitisation.

NodeZro's Principles of Classification

The NodeZro Identity Impact Taxonomy is built upon four fundamental principles that guide the classification and potential impact of findings. These principles provide a structured approach for prioritising the remediation of findings. By adhering to this approach, organisations can ensure they address the most urgent and important threats first, thereby optimising their efforts in safeguarding their digital identities, revenues and reputation. This proactive stance helps maintain the trustworthiness of their brands, ensuring that the integrity of their digital identity remains intact.

Principle 1 - Complete Traffic Breach and Full Identity Control

Findings pertaining to identities that are already breached or demonstrate the potential to be breached for both incoming and outgoing traffic, are accorded the highest urgency level. This is because an attacker can potentially exert full control over that identity, These findings signify the most acute risk as they are capable of causing severe operational disruption, breaching regulations such as the General Data Protection Regulation (GDPR) (5) and/or the California Consumer Privacy Act (CCPA) (12), damaging a brand's reputation, and may enable malevolent entities to assume control over the brand's identity.

Principle 2 - Outbound Traffic Breach and Partial Identity Control

Findings that could breach and control a brand's outbound traffic and enable partial control over the identity, such as those enabling identity spoofing via missing or faulty Domain-based Message Authentication, Reporting and Conformance (DMARC) (6) records, are considered serious, although not as severe as findings that can breach traffic in both directions. Nevertheless, they demand immediate attention to prevent potential misuse of the brand's identity.

Principle 3 - Service Availability and Hygiene

Findings that are unlikely to result in traffic breaches in either direction, yet could affect service availability, leak configuration information or compromise identity hygiene, are considered less severe. This Principle includes findings such as domain names that resolve to IPs of internal systems, potentially revealing sensitive internal infrastructure details. It also includes DNS servers configured to permit DNS zone transfers (AXFR) (15). Misconfigurations that compromise redundancy are also identified under this principle. Such misconfigurations can weaken an organisation's resilience to service disruptions and attacks, like Denial of Service (DoS) (13) threats. Although these findings may not directly threaten a brand's core identity, they could detrimentally affect service quality and security. Untreated, they can lead to significant financial implications, long-term damage, and erosion of brand trust and reputation.

Principle 4 - Informational and Recommendation Findings

Findings that include recommendations and advisories are classified as informational. Generally, they are not seen as threats but offer valuable guidance to improve the overall resilience and redundancy of a brand's digital identity management.

	Extensive Impact	Moderate Impact	Minor Impact
High Urgency	Principle 1	Principle 2	
Medium Urgency		Principle 3	
Low Urgency			Principle 4

Table 1: Mapping Principles to Urgency and Impact

Purpose and Scope of the Taxonomy

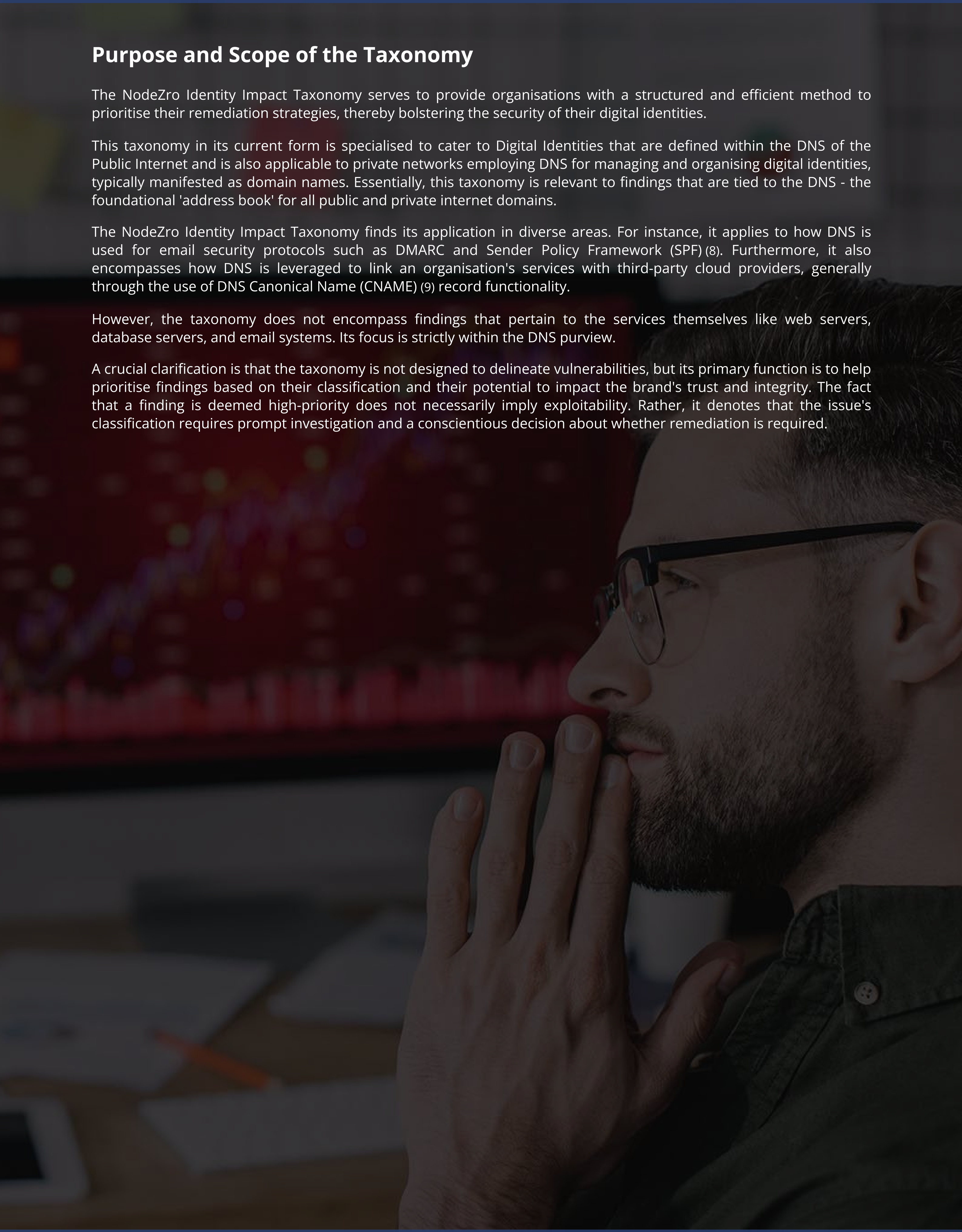
The NodeZro Identity Impact Taxonomy serves to provide organisations with a structured and efficient method to prioritise their remediation strategies, thereby bolstering the security of their digital identities.

This taxonomy in its current form is specialised to cater to Digital Identities that are defined within the DNS of the Public Internet and is also applicable to private networks employing DNS for managing and organising digital identities, typically manifested as domain names. Essentially, this taxonomy is relevant to findings that are tied to the DNS - the foundational 'address book' for all public and private internet domains.

The NodeZro Identity Impact Taxonomy finds its application in diverse areas. For instance, it applies to how DNS is used for email security protocols such as DMARC and Sender Policy Framework (SPF) (8). Furthermore, it also encompasses how DNS is leveraged to link an organisation's services with third-party cloud providers, generally through the use of DNS Canonical Name (CNAME) (9) record functionality.

However, the taxonomy does not encompass findings that pertain to the services themselves like web servers, database servers, and email systems. Its focus is strictly within the DNS purview.

A crucial clarification is that the taxonomy is not designed to delineate vulnerabilities, but its primary function is to help prioritise findings based on their classification and their potential to impact the brand's trust and integrity. The fact that a finding is deemed high-priority does not necessarily imply exploitability. Rather, it denotes that the issue's classification requires prompt investigation and a conscientious decision about whether remediation is required.



NodeZro Urgency-Impact Prioritisation Matrix

The NodeZro Identity Impact Taxonomy serves as a valuable guide to streamline workflow and elevate the effectiveness of digital identity management. By categorising findings and prioritising them accordingly, the taxonomy helps allocation of resources and attention based on the context and potential impact of each finding.

The taxonomy recognises that each finding has its own unique context and significance. It emphasises the importance of understanding and addressing findings within their specific context to reinforce the security and trustworthiness of corporate digital identity.

NodeZro employs two key metrics to evaluate and assign the priority of Identity Impact: Impact itself, and Urgency:

- ### Impact

  Impact is a measure of the potential effect of a finding on an organisation should the issue or vulnerability be exploited. In the context of a corporate digital identity breach, the resulting impact can manifest in numerous ways, affecting a wide array of business elements. Impact can encompass several facets of a business, from its brand value, reputation, and customer satisfaction to more tangible aspects like its share price, financial cost, loss of revenue, or the effort (person hours) required to resolve the issue.

  NodeZro stratifies impact into three categories:

  Extensive Impact: These are scenarios where the effect of a breach could significantly harm an organisation's operations and reputation. An extensive impact could lead to substantial financial losses, a significant drop in share price, severe damage to the brand's reputation, and major customer dissatisfaction. The resolution might require substantial resources, time, and effort, and there could be long-term ramifications even after the problem is resolved.

  Moderate Impact: This level of impact denotes incidents where the effects of the breach are substantial but not crippling. There could be financial losses, but they are manageable; the reputation might take a hit, but it's recoverable; customers might be displeased, but not to the point of mass desertion. The effort to resolve the issue is significant, but the business can recover without long-lasting negative effects.

  Minor Impact: These are instances where the effect of a breach is limited and manageable. Financial losses, if any, are minimal; there might be a temporary dip in customer satisfaction or a slight knock to the reputation, but both are quickly rectified. The effort required to resolve the issue is reasonable and within the scope of regular business operations, without causing major disruptions or long-term damage.

- ### Urgency

  Urgency, as distinct from impact, is not about the potential effect of a vulnerability or an incident but more about the rate of response needed. It reflects the timeframe within which an organisation and its stakeholders would expect an issue to be addressed. This could involve reinstating a service to normal operation or formulating, implementing, and delivering a solution or remedy.

  NodeZro categorises urgency into three levels:

  High Urgency: These situations necessitate immediate response due to the severity of the potential damage or the short window for resolution. They may represent instances where every moment of delay might compound the potential consequences, escalate the situation, or increase the risk of the issue becoming unmanageable. High urgency matters might include severe security breaches, acute operational outages, or situations that may result in immediate and substantial financial loss or legal liability.

  Medium Urgency: This level of urgency applies to cases where the need for action is pressing but not instantaneous. There's a window of time, albeit limited, to react and mitigate the issue before it escalates significantly. Issues of medium urgency might include minor operational disruptions, lesser security concerns, or potential customer dissatisfaction which, if left unattended, could worsen over time.

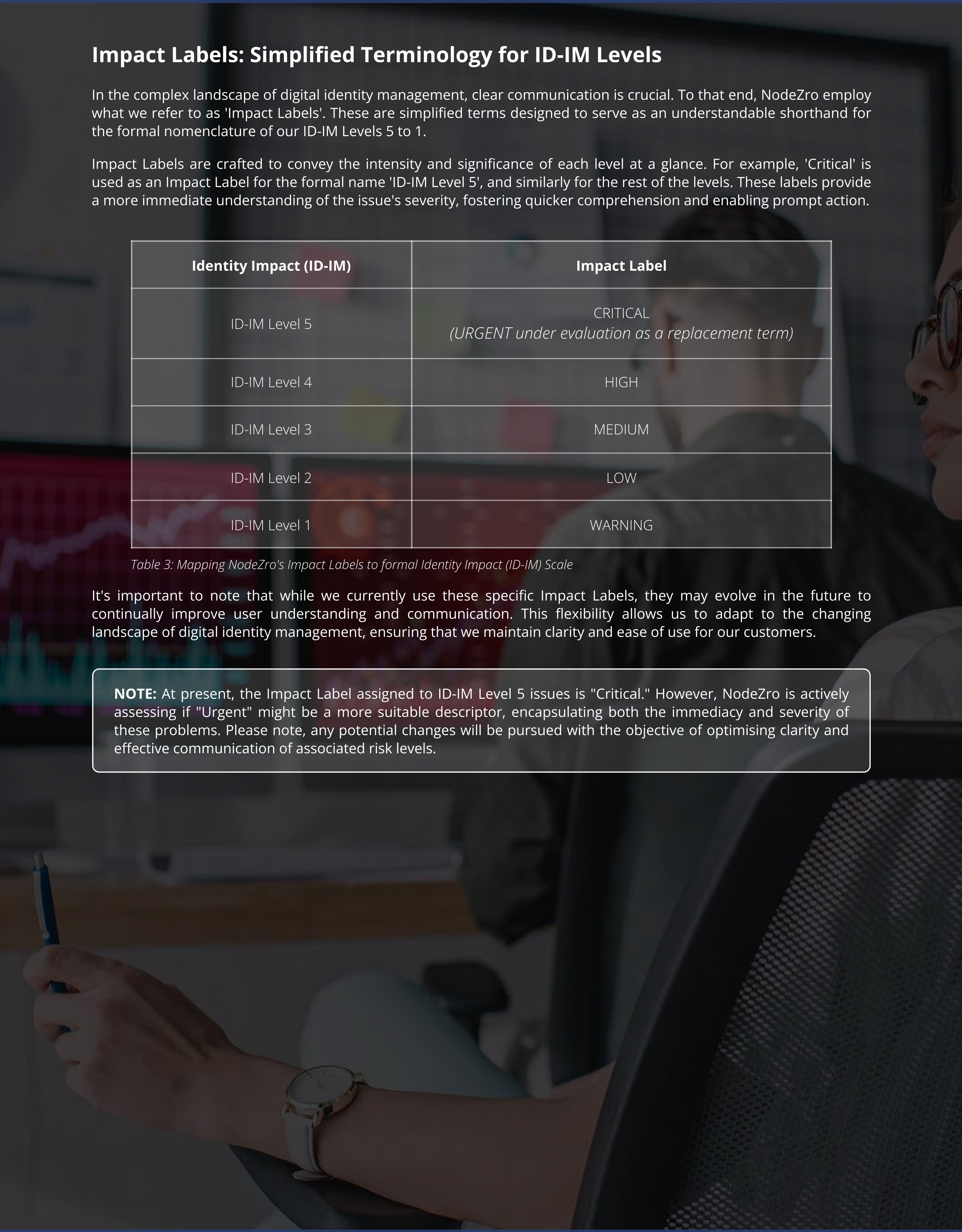
  Low Urgency: These cases signify situations where the requirement for action, while still present, is not immediate. There's ample time to assess the situation, plan the appropriate response, and apply a remedy without the fear of significant escalation or immediate damage. Low urgency matters could encompass non-critical operational findings.

The Urgency-Impact Matrix

The interplay of Impact and Urgency gives rise to the prioritisation matrix. Each finding is plotted on this matrix, based on its respective urgency and impact. The position of the finding on the matrix dictates the priority level for addressing it, helping organisations to effectively manage their digital identity risks and strengthen their overall digital security posture.

NodeZro Identity Impact		**Impact**		
		1 - Minor	2 - Moderate	3 - Extensive
Urgency	2 - High	3	4	5
	1 - Medium	2	3	4
	0 - Low	1	2	3

Table 2: How Urgency and Impact is mapped to NodeZro Identity Impact (ID-IM) Scale



Impact Labels: Simplified Terminology for ID-IM Levels

In the complex landscape of digital identity management, clear communication is crucial. To that end, NodeZro employ what we refer to as 'Impact Labels'. These are simplified terms designed to serve as an understandable shorthand for the formal nomenclature of our ID-IM Levels 5 to 1.

Impact Labels are crafted to convey the intensity and significance of each level at a glance. For example, 'Critical' is used as an Impact Label for the formal name 'ID-IM Level 5', and similarly for the rest of the levels. These labels provide a more immediate understanding of the issue's severity, fostering quicker comprehension and enabling prompt action.

Identity Impact (ID-IM)	Impact Label
ID-IM Level 5	CRITICAL *(URGENT under evaluation as a replacement term)*
ID-IM Level 4	HIGH
ID-IM Level 3	MEDIUM
ID-IM Level 2	LOW
ID-IM Level 1	WARNING

Table 3: Mapping NodeZro's Impact Labels to formal Identity Impact (ID-IM) Scale

It's important to note that while we currently use these specific Impact Labels, they may evolve in the future to continually improve user understanding and communication. This flexibility allows us to adapt to the changing landscape of digital identity management, ensuring that we maintain clarity and ease of use for our customers.

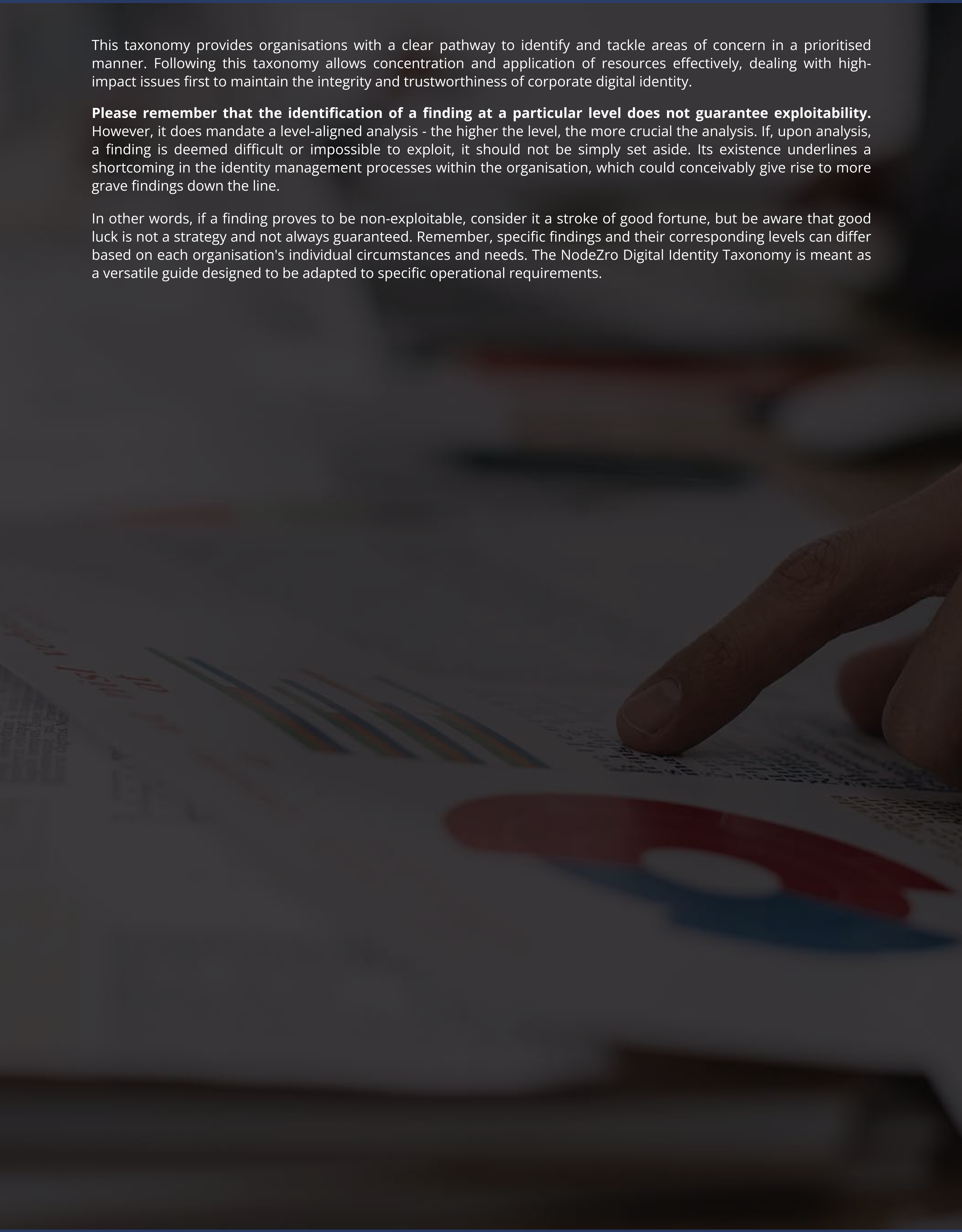
NOTE: At present, the Impact Label assigned to ID-IM Level 5 issues is "Critical." However, NodeZro is actively assessing if "Urgent" might be a more suitable descriptor, encapsulating both the immediacy and severity of these problems. Please note, any potential changes will be pursued with the objective of optimising clarity and effective communication of associated risk levels.

Mapping NodeZro's Principles for Digital Identity Management to the ID-IM Scale

The following table illustrates how NodeZro's Principles of Classification align with the ID-IM scoring system.

Category	NodeZro's Principles for Digital Identity Management
ID-IM 5	The results at this level could potentially lead to a complete breach of traffic and full control of an organisation's identity, following Principle 1. This can have an instant and disastrous effect on an organisation. Findings at this level often involve scenarios where the identity of the organisation has already been compromised. Findings at this level include linked suppliers that are no longer operational or digital identities pointing to resources within open namespaces that can be easily exploited. Open namespaces, such as those listed on the Public Suffix List (PSL)(10), pose a significant risk as they may be accessible to anyone, including potential malicious actors. Evaluating ID-IM 5 findings is crucial because even if a specific finding within this category is not immediately exploitable, its mere presence indicates a critical flaw in the digital identity management processes of an organisation.
ID-IM 4	Findings at this level carry the potential for serious consequences, such as a full-scale traffic breach and complete control over an organisation's identity in line with Principle 1. These outcomes can cause immediate and severe harm to an organisation. Should digital identities link to resources that no longer respond, yet are not explicitly included in the Public Suffix List (PSL) or a Top-Level Domain (TLD), these would be classified in this category. These identities continue to present a considerable risk due to their potential exploitation through service providers. This is common among certain cloud service providers where previously used resources that have been abandoned can subsequently be reappropriated by third parties, thereby compromising an organisation's digital identity.
ID-IM 3	At this level, findings could potentially breach an organisation's outbound traffic and gain partial control over its identity in line with Principle 2. These findings are serious, albeit not as critical as situations indicating a bi-directional traffic breach. However, they still warrant prioritised analysis and intervention to avert any potential misuse of the organisation's identity. These findings serve as indicators that digital identity management processes need strengthening. By addressing these significant findings, the security and integrity of outgoing traffic can be enhanced, reducing the risk of spoofing and unauthorised use of corporate digital identity.
ID-IM 2	At this level, the findings typically don't pose a direct threat of breaching traffic either inbound or outbound in line with Principle 3. However, they may influence service availability, leak configuration information or relate to identity hygiene. These findings are deemed less severe but are not to be overlooked. Although they don't directly endanger a brand's identity, they could potentially reduce service quality and inflict long-term harm if left unattended.
ID-IM 1	At this level, findings generally consist of recommendations and advisories, and are classified as informational in line with Principle 4. While they typically don't pose direct threats, they offer valuable insights to enhance the overall robustness and backup systems of an organisation's digital identity management.

Table 4: Mapping NodeZro's Principles to the Identity Impact (ID-IM) Scale



This taxonomy provides organisations with a clear pathway to identify and tackle areas of concern in a prioritised manner. Following this taxonomy allows concentration and application of resources effectively, dealing with high-impact issues first to maintain the integrity and trustworthiness of corporate digital identity.

Please remember that the identification of a finding at a particular level does not guarantee exploitability. However, it does mandate a level-aligned analysis - the higher the level, the more crucial the analysis. If, upon analysis, a finding is deemed difficult or impossible to exploit, it should not be simply set aside. Its existence underlines a shortcoming in the identity management processes within the organisation, which could conceivably give rise to more grave findings down the line.

In other words, if a finding proves to be non-exploitable, consider it a stroke of good fortune, but be aware that good luck is not a strategy and not always guaranteed. Remember, specific findings and their corresponding levels can differ based on each organisation's individual circumstances and needs. The NodeZro Digital Identity Taxonomy is meant as a versatile guide designed to be adapted to specific operational requirements.

Identity Exposure Score

NodeZro has designed a comprehensive scoring system that assesses the relative risk or 'Identity Exposure' of each entity within its taxonomy. This system produces both a raw score and a comparative index, allowing for detailed analysis of an individual entity's exposure as well as comparisons between different entities and baseline averages.

Scoring Process

The scoring system is built upon a multi-level structure, wherein each level is assigned a score that diminishes progressively down the levels. This graduated scoring ensures that more severe issues have a higher impact on the overall exposure index.

Scoring Levels and Calculation

NodeZro's scoring model is based on five levels, with each level assigned a score that decreases progressively as it moves from Level 5 down to Level 1. The highest level (Level 5) is assigned a base score of 100.

From there, the score for each subsequent level is calculated as the score of the preceding level divided by 5. The rationale for this factor is discussed below. Here's how the scores are calculated for each level:

Level	Calculation	Score
ID-IM Level 5	100	100
ID-IM Level 4	100/5	20
ID-IM Level 3	100/5/5	4
ID-IM Level 2	100/5/5/5	0.8
ID-IM Level 1	100/5/5/5/5	0.16

Table 5: Identity Exposure Score and Calculations.

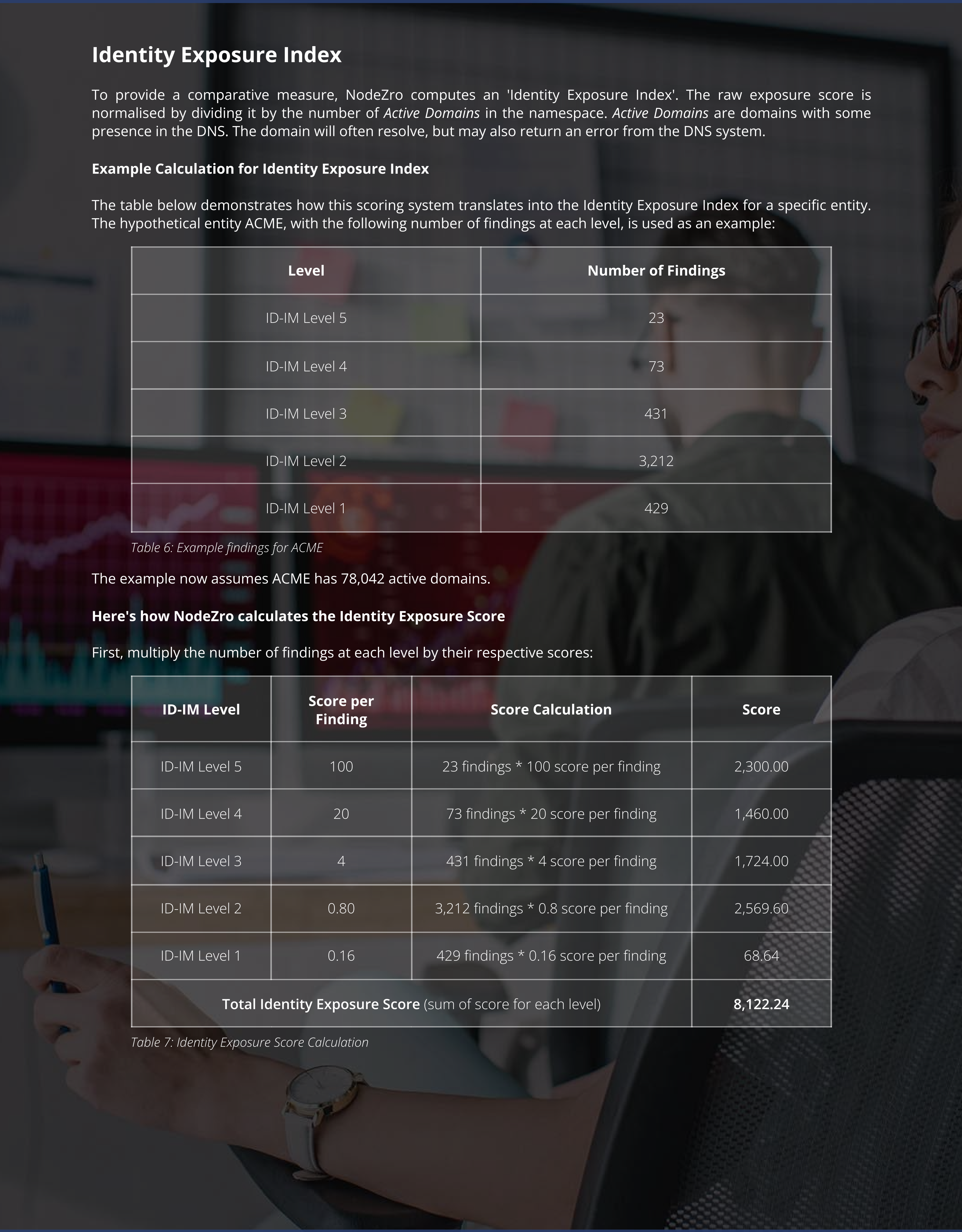
As evident from the table, a finding at Level 3 will contribute less to the overall Exposure Score than a Level 4 finding, due to the diminishing score as it descends through the levels. This scheme ensures that severe issues at higher levels significantly impact the final exposure score, effectively highlighting them for their appropriate Impact and Urgency.

Rationale Behind the Scaling factor

NodeZro's selection of 5 as the scaling factor aligns with its assessment of the relative impacts between various levels of findings. This scaling factor ensures that severe issues are given appropriate weight in the final exposure index.

The scaling factor of 5 was chosen based on careful consideration and analysis of the relative severity and impact of issues across the five levels of NodeZro's taxonomy. It allows for a clear distinction between each level, effectively emphasising the importance and urgency of higher-level findings.

This number reflects the fact that issues classified at level 5 are expected by NodeZro to be approximately five times as important as those at level 4, and so on. This scale mirrors assessments of relative impact and urgency and creates a weighted system where serious issues contribute significantly more to the overall Identity Exposure Index.



Identity Exposure Index

To provide a comparative measure, NodeZro computes an 'Identity Exposure Index'. The raw exposure score is normalised by dividing it by the number of *Active Domains* in the namespace. *Active Domains* are domains with some presence in the DNS. The domain will often resolve, but may also return an error from the DNS system.

Example Calculation for Identity Exposure Index

The table below demonstrates how this scoring system translates into the Identity Exposure Index for a specific entity. The hypothetical entity ACME, with the following number of findings at each level, is used as an example:

Level	Number of Findings
ID-IM Level 5	23
ID-IM Level 4	73
ID-IM Level 3	431
ID-IM Level 2	3,212
ID-IM Level 1	429

Table 6: Example findings for ACME

The example now assumes ACME has 78,042 active domains.

Here's how NodeZro calculates the Identity Exposure Score

First, multiply the number of findings at each level by their respective scores:

ID-IM Level	Score per Finding	Score Calculation	Score
ID-IM Level 5	100	23 findings * 100 score per finding	2,300.00
ID-IM Level 4	20	73 findings * 20 score per finding	1,460.00
ID-IM Level 3	4	431 findings * 4 score per finding	1,724.00
ID-IM Level 2	0.80	3,212 findings * 0.8 score per finding	2,569.60
ID-IM Level 1	0.16	429 findings * 0.16 score per finding	68.64
Total Identity Exposure Score (sum of score for each level)			**8,122.24**

Table 7: Identity Exposure Score Calculation

Finally, to arrive at the Identity Exposure Index, divide the Total Identity Exposure Score by the number of active domains in ACME's namespace:

Total Identity Exposure Score	Number of Active Domains	Identity Exposure Index Calculation	Identity Exposure Index
8,122.24	78,042	8,122.24 / 78,042	**0.1041**

Table 8: Total Identity Exposure Score Calculation

The Identity Exposure Index for ACME, given these example numbers, is approximately 0.1041. This index value represents the normalised measure of ACME's exposure based on NodeZro's scoring model and the size of ACME's active domain portfolio.

NOTE: It's important to bear in mind that the count of Active Domains might require normalization in instances where wildcard records exist within a namespace. Such wildcard records can potentially inflate the count of active domains, representing a higher number than those that are genuinely in use. Consequently, this can skew the Identity Exposure Index score, making it seem higher than it should be. It is recommended to account for these wildcard records when assessing the index score to ensure accurate and meaningful comparisons.

Identity Exposure Index comparison to Baseline:

The Identity Exposure Index for ACME is calculated to be 0.1041. NodeZro has a range of baselines it uses to evaluate performance:

- **Global Baseline:** This metric encompasses a broad scope, capturing data across geographies and industries on a global scale, forming a comprehensive international average.
- **Geography Baseline:** This measurement represents aggregate data across a specific geographic region, establishing a localised average.
- **Industry Baseline:** This metric denotes a comprehensive analysis across a specific industry, thus creating an industry-specific baseline.
- **Local Baseline:** This metric represents a specialised assessment within a specific industry and geographic region, thereby establishing a regionally-focused industry baseline.
- **Supply Chain Baseline:** This metric uniquely corresponds to your own ecosystem, taking into account discovered suppliers involved in your operations. By calculating the Identity Exposure Index for each of these entities and averaging the results, a personalised baseline reflecting the security posture of your supply chain is established.

The process of calculating the Identity Exposure Index Baselines involves several key steps. Firstly, NodeZro computes the Identity Exposure Index for every participant included within the Baseline. This initial calculation phase forms the basis for the second step. Following this, we aggregate all the individual results and divide this total by the number of entries to obtain the average. Let's say, for instance, you have a supply chain composed of 321 suppliers. NodeZro will calculate the Identity Exposure Index for each of these 321 suppliers, sum up these results, and then divide this total by 321. This computation results in the average Identity Exposure Index for your supply chain, serving as your unique Supply Chain Baseline.

In this case the Supply Chain Baseline has been calculated as 0.092. Using this baseline figure ACME's performance in relation to this baseline can be compared.

Identity Exposure Index comparison to Baseline:

Entity	Identity Exposure Index	Performance against baseline	Result
ACME	0.1041	((0.092 - 0.1041) / 0.092)*100	-13.15% (↓)

Table 9: Identity Exposure Index comparison to Baseline

This means that ACME's Identity Exposure Index is approximately -13.15% lower than the global baseline. In other words, ACME is performing -13.15% worse than its peers in terms of Identity Exposure. This comparative analysis provides valuable insights into an entity's risk exposure relative to its peers or industry averages. The Identity Exposure Index thus serves as a crucial tool for assessing and managing digital identity risk.

Taxonomy Examples

CATEGORY	IMPACT TYPE	EXAMPLES
ID-IM 5	Identity has already been breached. Complete Traffic Breach and Full Identity Control. Impact may include significant decline in an organisation's value or Market Cap. Research has found a decline in Market Cap of 7.5% for organisations that experience a significant breach (3).	**Example 1: Urgency = High and Impact = Extensive** A canonical name record (CNAME) for the domain (alias) “example.com” is pointing to a domain which is hosted on the nameservers of a domain name parking company. This supply chain vulnerability is a strong indication that the primary domain is available for sale and may be acquired by anyone at any time. Corporate identity is breached and is currently under the control of an unauthorised third party. It has been left unmanaged due to a lack of lifecycle management and action must be taken to reconfigure or decommission. **Example 2: Urgency = High and Impact = Extensive** A dangling canonical name record (CNAME) for the domain (alias) “node.example.com” is pointing to an external domain “external.example.net” that no longer exists and where the organisational domain returns DNS RCODE (3) NXDOMAIN. This is a strong indication that the domain may be available to anyone at any time and could allow someone to take control of the domain name “node.example.com”. An organisational domain is defined as a domain that's on the Public Suffix List (PSL) (10), but which isn't directly in a Top Level Domain (TLD) (11). These domains may or may not be available for registration depending upon the namespace. A manual review is required to establish how easy the issue is to exploit. Identity is linked to a third party domain that may not be under corporate control. It is at very high risk of compromise, putting corporate and stakeholder information at risk. This identity has been left unmanaged and should be considered for reconfiguration or decommissioning.
ID-IM 4	Complete Traffic Breach and Full Identity Control.	**Example 1: Urgency = Medium and Impact = Extensive** A dangling canonical name record (CNAME) for the domain (alias) “example.com” is pointing to an external domain “example.net” that no longer exists. If a third-party can take control of the domain name “example.net”, they may be able to control “example.com”. Identity linked to a third party domain that may not be under corporate control. It is at high risk of compromise, putting corporate and stakeholder information at risk. This identity has been left unmanaged and should be considered for reconfiguration or decommissioning. **Example 2: Urgency = Medium and Impact = Extensive** A dangling Mail eXchanger Record (MX) is pointing to an external domain that no longer exists. This is a strong indication that the domain could be available to anyone at any time. This could allow anyone to take control of email services for the domain name “example.com”. Since the dangling domain is in an external namespace that may not be under corporate control, this finding is high risk and a manual review is needed to establish the full extent of the risk. Email is routed to a third-party abandoned email server that may not be under corporate control. Email for his identity is at high risk of compromise, leaving corporate and stakeholder information at risk. This identity has been left unmanaged and should be considered for reconfiguration or decommissioning.

Taxonomy Examples

ID-IM 3	Outbound Traffic Breach and Partial Identity Control	**Example 1: Urgency = Medium and Impact = Moderate** The domain “example.com” has MX records to accept email but is missing DMARC TXT records to protect the domain from unauthorised use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing emails and other cyber threat activities. This finding should be reviewed and remediated if appropriate. Identity's email services have not been safeguarded using the available mechanisms to protect against the unauthorised use of your email domains. **Example 2: Urgency = Medium and Impact = Moderate** The domain “example.com” has delegation and authoritative name server records (NS) that don't match. This is usually a moderate risk finding but in certain configurations can be a serious security risk. If a domain has different delegation and authoritative NS records and it's not by design, it can result in security issues. A manual review is needed to establish the full extent of the risk. Identity has mismatching configuration information and may have been misconfigured. Examine this identity to rule out any possibility of compromise or impact on services.
ID-IM 2	Service Availability and Hygiene	**Example 1: Urgency = Low and Impact = Moderate** The DNS response to an A record lookup for the domain “example.com” contains a private IP address. This may indicate a leak of internal domains and their IP addresses onto the public internet. This should be reviewed to determine if it's a hygiene issue or if it's by design. Identity could assist bad actors in mapping corporate internal infrastructure and systems. It is leaking information on internal systems onto the Internet. **Example 2: Urgency = Medium and Impact = Minor** The authoritative nameserver doesn't respond with an authoritative answer for the domain “example.com”. This means that one of the nameservers that's listed as authoritative for the domain “example.com” in the DNS is responding with a non-authoritative DNS answer. This finding is a variant of a class of DNS issues that are often referred to as lame delegations. Identity has a misconfiguration that may affect its services.

Taxonomy Examples

ID-IM 1	Informational and Recommendation Findings	**Example 1: Urgency = Low and Impact = Minor** The domain “example.com” is responding with TXT records for the “_dmarc.example.com” subdomain but returns multiple TXT records. This may or may not be an issue but could indicate a domain hygiene problem and should be reviewed. Identity is publishing unexpected information in the DNS and the information should be reviewed. **Example 2: Urgency = Low and Impact = Minor** The domain “example.com” has only one published mail exchanger (MX). This could be a resiliency finding and should be reviewed. Some providers like Microsoft (outlook.com) are known to only provide one MX, so this may be by design and not an issue of concern.

Table 10: Examples of how the ID-IM Scale is mapped to Findings

Sources

1. Bitglass.com: https://pages.bitglass.com/rs/418-ZAL-815/images/Bitglass_Kings_of_the_Monster_Breaches.pdf
2. The Devastating Business Impacts of a Cyber Breach (Harvard Business Review 2023): https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach
3. Companies' Stock Value Dropped 7.5% after Data Breaches (Infosecurity Magazine): https://www.infosecurity-magazine.com/news/companies-stock-value-dropped-1/
4. Adobe 2022 Trust Report: https://business.adobe.com/content/dam/dx/uk/en/resources/reports/adobe-trust-campaign-hub-page/pdf/2022_Trust_report_UK.pdf
5. Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504
6. DMARC: https://en.wikipedia.org/wiki/DMARC
7. Domain Name System (DNS): https://en.wikipedia.org/wiki/Domain_Name_System
8. Sender Policy Framework (SPF): https://en.wikipedia.org/wiki/Sender_Policy_Framework
9. Canonical Name (CNAME) record: https://en.wikipedia.org/wiki/CNAME_record
10. Public Suffix List (PSL): https://en.wikipedia.org/wiki/Public_Suffix_List
11. IANA Root Zone Database of Top Level Domains (TLDs): https://www.iana.org/domains/root/db
12. California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa
13. Denial-of-Service attack (DoS attack): https://en.wikipedia.org/wiki/Denial-of-service_attack
14. Software as a service (SaaS): https://en.wikipedia.org/wiki/Software_as_a_service
15. DNS zone transfer (AXFR): https://en.wikipedia.org/wiki/DNS_zone_transfer

About NodeZro Ltd

> NodeZro specialises in mapping, monitoring and securing large and complex Internet namespaces. NodeZro helps corporations and governments understand, sanitise and protect their vulnerable DNS networks across the globe. NodeZro LTD is a UK company with Company No. 13737105.

Disclaimer:
NodeZro Ltd is not liable for any damages arising in contract, tort or otherwise from the use of or inability to use this report or any material contained in it, or from any action or decision taken as a result of using this data. The materials in this report comprise the views of NodeZro Limited which, due to the nature of the data reported on, will always be incomplete and potentially inaccurate; they do not constitute legal or other professional advice. You should consult your professional adviser for legal or other advice. All product names, logos, brands, trademarks and registered trademarks are property of their respective owners. All company, product and service names used in this report are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement.

nodeZro
cyber intelligence solutions