Zero Trust Validation

J. Scheerder* Y. Bobbert*

December 24, 2019

1 Introduction

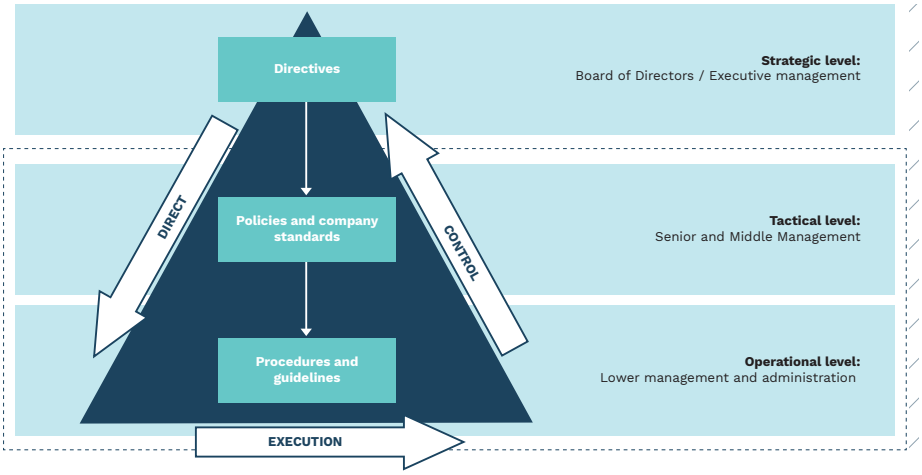
ON2IT advocates the Zero Trust conceptual strategy to strengthen information security at the architectural level. Zero Trust is often mistakenly perceived as an *architectural* approach. However, it is, in the end, a *strategic* approach towards protecting assets regardless of location.

To enable this approach, *controls* are needed to provide sufficient insight (visibility), to exert control, and to provide operational feedback. However, these controls/probes are not *naturally* available in all environments. Finding ways to embed such controls, and finding/applying them, can be challenging, especially in the context of containerized, cloud- and virtualized workflows.

1. Strategic level: Governance
2. Managerial level: Execution
3. Operational level: Operations

At the strategic level, Zero Trust is not sufficiently perceived as a value contributor. At the managerial level, it is perceived mainly as an architectural 'toy'. This makes it hard to translate a Zero Trust strategic approach to the operational level; there's a lack overall coherence.

For this reason, ON2IT developed a Zero Trust Readiness Assessment framework which facilitates testing the readiness level on three levels: governance, management and operations.



For example, to understand and fully grasp the context of your business environment and your own organi-

*ON2IT b.v., Waardenburg, The Netherlands.

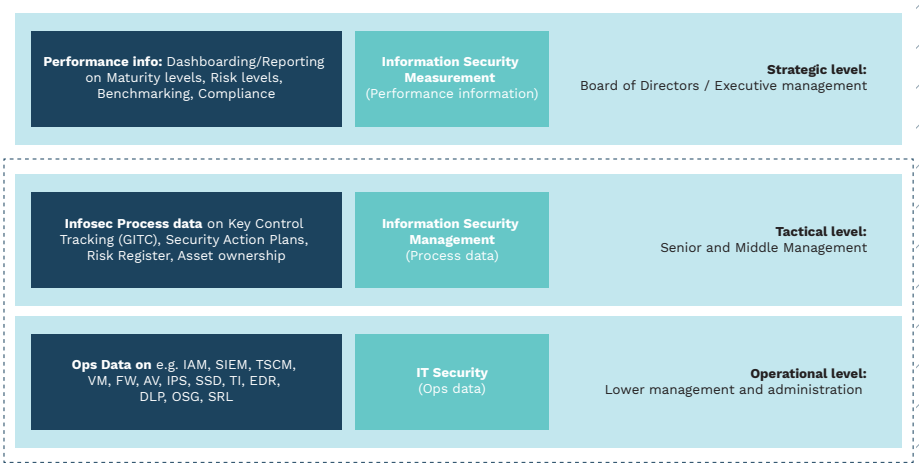
sation's capabilities, you need to assess multiple attributes: Business Risks, DAAS[1] Management, Ownership and Sign Off, Management Reporting on Zero Trust Progress.

At the managerial level, you check for Data Classification Ability, Requirement Analysis, Third-Party Risk Management, Change Management.

Operationally, test 'fitness' on technical capabilities: Micro-Segmentation (which can include virtual, container, cloud deployments), Presence of Sufficient Security Policy Controls, Deployment of Cryptography, Version Management, Orchestration and Automation, CI/CD Integration.

Assessing an organisations' posture with respect to Zero Trust viability requires evaluating these three levels, *and this ON2IT framework*. Ideally, we would like to propose four research areas:

1. Validation of the Zero Trust Readiness framework (pre- and post-implementation progress monitor);
2. Assessing the presence and relevance of strategic capability attributes (strategic level);
3. Assessing the presence and relevance of executive capability attributes (managerial Level);
4. Assessing the presence and relevance of adequate technical capabilities (operational level).



These assessments determine the relevance, coverage, depth and actionability of the controls/objectives (at their respective level).

[1]Data, Applications, Assets, Services.

2 Zero Trust R&D Assignment

2.1 Problem area

Improving and maintaining an adequate level of Business Information Security is cumbersome. The hybrid technology landscapes, war on talent and lack of real-time visibility in operations makes it hard for boards to take ownership and accountability of Cyberrisks.

Network perimeters dilute and smart devices make the entrance in an api-based ecosystems of organisations. For companies that are not tech-born Zero Trust architecture can solve the majority of the issues of; critical asset identification, user and device validation, access control mechanisms, traffic inspection, micro-segmentation, policy orchestration and enforcement, control validation, dashboarding and reporting that is needed for companies license to operate or their ticket to win deals.

2.2 Main research question

What is missing in the current approach of ZTA to make it resonate with the board?

Zero Trust, being predominantly practiced by technicians and architects, has gained little attention at senior management and board level. Companies like BCG, Accenture, Deloitte and EY developed and implemented their own internally developed approaches based upon accepted community frameworks like COSO for Enterprise Risk Management (ERM), COBIT for governing IT (Enterprise Governance of IT, EGIT) and ISO since its respected position in quality assurance in retail and industrial environments. The ISO27000 series is already a predominant factor in information security management when it comes to ensuring the Plan, Do, Check, Act cycle that is needed for maintaining an adequate improvement cycle and ISO27002 for the required security controls per domain. Since its introduction in 2010 Forrester put forward the thought leadership of John Kindervag in their approaches, mainly focusing on managerial level but lack operational detailing that DevOps teams and engineers can get proper guidance from. It also absence the required Governance practices that are needed. The complete connection between Boardroom and DevOps Teams is cumbersome and depends on a lot of organisation preconditions such as formal structures, processes and relational mechanisms to effectively embrace the Zero Trust philosophy as a strategic approach rather than the current ad-hoc architectural approach. Thus, what is missing in the current approaches is:

Board involvement since ZeroTrust is perceived as an architectural "toy" concealed with mystique and a lot of technical jargon without clear business goals alignment, guidance, metrics and outcomes. According to NIST (2019) publications it also misses a common framework –or alignment with existing frameworks- and a common vocabulary. This works both ways thus also bards need to know what knowledge and capability are required[2]. Ownership of assets and risks, due to rotation of personnel, introduction of new tech-services without IT involvement, formal procurement processes (vendor vetting etc), mergers and acquisitions, rough and orphan assets become the new standard rather than an exception. Let alone an adequate Configuration Management DataBase (CMDB) is presence. However proper administration of critical assets, their value, classification of the housed data, CIA ratings etc is not in place nor centrally administered[3]. Single pane of glass e.g. complete visibility over multiple point solutions that do "something with risk, security, compliance" . This wood of security tools enables decision latency[4] due to inefficient security operations that has limited interaction since the tools are owned, consumed, managed and measured by multiple actors e.g. auditors, IT managers, security staff, business users.

[2]Hooper et al. states "organisations need to embrace their concern about cybersecurity and build it into their selection criteria for board members".

[3]Bobbert, 2019, *LockChain technology as one source of truth for Cyber, Information Security and Privacy*.

[4]The Standish Group: Decision latency theory states: "The value of the interval is greater than the quality of the decision." Therefore, to improve performance, organisations need to consider ways to speed-up their decisions.

2.3 What are Critical Success Factors for drafting and implementing ZTA?

When looking at the current Zero Trust implementations the majority of the work was put into aligning all stakeholders to the strategy of Zero Trust. The CISO of a large global firm quotes "I have spend the majority of the time in taking operational and tactical personnel on board of my journey and convince them this would be a long one". "And I needed to make sure I had appropriate ownership for critical assets and services in the company since these assets owners had to be involved in determining the critical value of the assets for a certain process". Since IT is not the owner of the asset, the business entity is so they are required for the dialogue to determine the type and level of controls. In other implementations we see the following Critical Success Factors needed before and during the ZeroTrust Journey of the implementation:

- Engage relevant stakeholders on the value of ZeroTrust for the business (e.g. proven control, reduce risk, decrease security spendings, strengthen Trust position[5] and the journey that lays in front of them. Since ZT is not simply switching the button. The role of the CISO is vital here[6].
- Alignment with existing control framework and their scaling, metrics and taxonomy so it enables collaboration between second-line risk managers and thirdline auditors have a common taxonomy, control objectives, Test of Design/Effectiveness, metrics, goals and perceived outcomes.
- Complete and accurate administration of critical assets (Data, Assets, Applications, Services) their economic value, CIA rating and their security requirements in a central repository (one source of truth).
- Clear technology roadmap with Zero Trust based measures that have a clear definition of done and timelines for implementation and test of the Design and Effectiveness via existing Governance and reporting processes.

Due to practical experiences we see that the most important factor for ZT success is to start with testing the organisations readiness and technological fitness to adopt and execute Zero Trust.

For this reason ON2IT developed a Framework. A unique Framework + Tools which consist of:

- Readiness assessment to determine how ready and fit you are as a company
- Maturity assessment to determine your level compared to objectives and peers
- Progress Monitor to report to boards and regulators
- Build in On2IT Cybersecurity platform Portal (reffered to as an *artefact*[7])

2.4 Zero Trust at the Strategic Level: Know Your Environment and Capabilities

At the Governance level, the following question needs to be addressed:

What is an easy to consume capability maturity or readiness model for the adoption of ZTA that guides boards and management teams in making the right decisions?

Subquestions:

- To what extend are the defined questions in the readiness assessment relevant for board members?

[5]Hooper et al. states "organisations need to embrace their concern about cybersecurity and build it into their selection criteria for board members".

[6]The CISO is generally the "heart and soul" of an information security program in most organisations. There is no better way to obtain a pulse regarding cyber risk" according to the International Audit Association.

[7]Yuri Bobbert, *On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering*, in: International Journal of IT/Business Alignment and Governance Vol. 8 Issue 2, 2017, https://www.igi-global.com/article/on-exploring-research-methods-for-business-information-security-alignment-and-artefact-engineering/189069.

- To what extend do they appeal to boardroom level language and main dilemma's?
- What topics are missing according to board members in the framework and portal?
- What is the main target group to use the assessment or to tak the assessment?
- Who on this level is consuming the dashboard data and for what reasons?

2.5 Zero Trust at the Managerial Level: Know Your Risk

At the Managerial level, the following question needs to be addressed:

What does a management portal with associated KPIs need to offer in order to enable board and management to manage and monitor the ZTA implementation process and take appropriate ownership?

Subquestions to validate the ZT assessment:

- To what extend are the defined questions in the readiness assessment relevant for management level? To gain better insight if the ZT approach appeals to business, security and IT management (as 3 different persona's)
- What topics are missing according to business, Security and IT management in the framework and portal?
- Who on this level is consuming the dashboard data and for what reasons?

2.6 Zero Trust at the Operational Level: Master Your Technology

At the Operational level, the following question needs to be addressed:

How do we add the necessary controls and leverage control and monitoring facilitities thusly provided efficiently?

Classically, networks were built as islands of closely connected systems, separated by an explicit boundary. The notion of 'perimeter security' flows naturally from this blueprint. Inspection and enforcement typically takes place at 'north/south' boundaries.

A slew of controls has arisen, allowing deep visibility into, and control over, network traffic by adding inspection- and enforcement capacilities at network boundaries: protocol validatin, threat detection, application detection/enforcement, user-identification and RBAC-based network access policy, URL categorisation and category-based access policy, and so on.

In virtual, container, cloud deployments there may not be a 'natural' boundary, where the desired controls can easily be allocated. Traffic might just as well be 'east/west', while still being subject (conceptually) to full policy enforcement.

Finding a way to enrich such deployments with the necessary controls, then, is the key question.

- How to embed full network security controls for 'east/west' traffic in virtual environments? With that control objective(s) are these controls aligned?
- How to add such controls in container environments? With that control objective(s) are these controls aligned?
- How to add such controls to cloud environments — brandX, brandY, ...? With that control objective(s) are these controls aligned?
- How to provision/orchestrate these control mechanisms and their policy? With that control objec-

tive(s) are these controls aligned?

Category	Controls	Description	ZTX Capabilities	Tools for control and/or implementation
Encryption	SSL Inbound Decryption	Decryption of traffic where you own the private key.	Data, Workload, Network	PAN FW
	SSL Outbound Decryption	Decryption of traffic where you don't own the private key.	Data, Workload, Network	PAN FW, Proxy
	Encryption at rest	Data not being used is encrypted	Data	Prisma Cloud
	Encryption in Transit	Data flowing through the network is encrypted	Data, Workload, Network	PAN FW, Prisma Cloud
IAM / UserID	Centrally managed IAM (one source of truth)	There is just one single source of truth for users.	People/Workforce	Questionnaire
	RBAC Based controls	User access is based upon roles.	People/Workforce	PAN FW
	MFA	Multifactor authentication is being used	People/Workforce	PAN FW
	Auditable (userID - logging)	Every log-rule can be related to a user	People/Workforce	PAN FW
(D)DOS	Volume Attacks (i.e. zone-protection)	Protection against large volume attacks (i.e. udp syn floods)	Network	PAN FW
	Targeted attacks (i.e. Policies)	Protection specific flows between clients and servers	Network	PAN FW
Endpoint	Exploit Prevention	Endpoints are protected against exploits	Device	Traps
	Malware prevention	Endpoints are protected against malware	Device	Traps
	Ransomware/Cryptolocker protection	Ransomware/cryptolockers can be detected and stopped	Devic,Workload,Data	Traps
	Central management	Devices are centrally managed and controlled	Device	Airwatch
Traffic flows	Segments	Segments can and are created to control traffic flows	Network, Data, Workload	PAN FW
	Restricted outbound access	Outbound access (outside security boundary) is strictly controlled	Network, Workload	PAN FW
	Restricted inbound access	Per segment there are strict controls for inbound access	Network, Workload	PAN FW
	Application based/controlled	Traffic policies are based on applications	Network	PAN FW
	Content-inspection	All flowing traffic is inspected (IDS/IPS)	Network, Data, Workload	PAN FW, Traps
	URL based	There are strict URL/URI policies in place	Network, Workload	PAN FW
	Behavioral analytics	Abnomalities on 'normal' flows can be detected	Network, Workload, Analytics and Automation	Cortex XDR
			Analytics	Questionnaire
Data	Credential Phishing prevention	Users leaking credentials can be detected and prevented	People/Workforce	PAN FW
	DLP controls are in place	Data leakage can be detected	Data	PAN FW, Prisma SaaS
	Data classification	Data is (and will be) classified	Data	Prisma SaaS
	Data discovery	Data can be discovered and classified	Data, Workload	Prisma SaaS, Prisma Cloud
	Data/Applications have their own segment	Every data/application has its own segment and is managed (CMDB)	Data, Workload	SAOP, PAN FW
Orchestrate/Automate	Rules of Engagement	Automatic actions can/will be taken on events	Analytics and Automation, Workload	SAOP
	State validation	The operational state can be matched against the designed state	Analytics and Automation, Workload	Prisma Cloud, Terraform
	Central policy management	Policies are centrally managed and enforced across different technologies	Analytics and Automation	Daryl?
Reporting	KRI, KPI	Key risk and performance indicators are in place and used for improvement	Analytics and Automation	SOAP

A References

- ISF framework (2019)
- Michel Modderkolk (2018), *ZERO TRUST MATURITY MATTERS: MODELING CYBER SECURITY FOCUS AREAS AND MATURITY LEVELS IN THE ZERO TRUST PRINCIPLE*
- Yuri Bobbert, *On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering*, in: International Journal of IT/Business Alignment and Governance Vol. 8 Issue 2, 2017, https://www.igi-global.com/article/on-exploring-research-methods-for-business-information-security-alignment-and-artefact-engineering/189069
- Ward, R., & Beyer, B. (2014). *BeyondCorp: A new approach to enterprise security*, Usenix Login, 39(6), 6–11.
- White, G. B. (2011). *The community cyber security maturity model*, 2011 IEEE International Conference on Technologies for Homeland Security, HST 2011, 173–178. http://doi.org/10.1109/THS.2011.6107866
- Kindervag, J. (2010a). *Build Security Into Your Network ' s DNA: The Zero Trust Network Architecture*
- Kindervag, J. (2010b). *No More Chewy Centers : Introducing The Zero Trust Model Of Information Security*
- Kindervag, J., Balaouras, S., Holland, R., & Blackborow, J. (2015). *Five Steps To A Zero Trust Network*
- Kindervag, J., Ferrara, E., Holland, R., & Shey, H. (2013). *The National Institute of Science and Technology: Developing a Framework to Improve Critical Infrastructure, (The National Institute of Science and Technology (NIST) within the Department of Commerce (Commerce))*, 1–18.
- Kindervag, J., Shey, H., & Mak, K. (2014). *The future of data security: A zero trust approach*

B About ON2IT R&D

Within the ON2IT CISO department continuous Research and Development is being done in the domains of cyberrisk, quantification, data analytics, artificial Intelligence, automation, orchestration, response techniques and validation.

The objective of the R&D team is to design and construct artefacts that solve the cyber problems at hand and contribute in optimal cybersecurity services towards our customers. By making use of Design Science Research methods we aim to build relevant technology with academic rigor. We do this in close collaboration with international tech vendors, regulatory bodies, hacking communities, corporations and universities. We neglect hypes and FUD and we strive to master the wicked cyber-problems. We combine passion for Cyber, research and engineering. With our R&D team we aim to build technology services that make impact on society *with* talented people that *want* to make impact and can have impact.

Those interested can contact Yuri Bobbert at Yuri.Bobbert@on2it.net.

ON2IT B.V.
Regterweistraat 7
4181 CE Waardenburg
The Netherlands

☎ +31 88 22 66 200
https://on2it.net
info@on2it.net
KvK 11062209