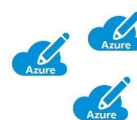




1

Agenda

- Let's Introduce Ourselves
- NN's Cloud Journey So Far
- The Future State of Cloud at NN
 - Boundaries
 - Guardrails
- Lessons Learned



2

2

Leon Kortekaas

Manager CIO/Cloud Integration at NN Group



Contact: Leon.Kortekaas@nn-group.com / <https://nl.linkedin.com/in/leonkortekaas>

3

3

Thomas Buiks

Product Owner Cloud Integration - Azure Team at NN Group



LEONIDAS



Contact: Thomas.Buiks@nn-group.com / <http://www.linkedin.com/in/thomasbuiks>

4

4

Renate Hendriksen

Cloud engineer – AWS team NN Group



gemeente Bronckhorst



university of
 groningen

CALCO
 IT'S THE WAY WE DO IT



NN

- AWS Cloud engineer
- Security Officer central IT



Contact: Renate.Hendriksen@nn-group.com / <http://www.linkedin.com/in/renatehendriksen>

5

5



Cloud Journey



6

6

International financial services company with strong businesses in Europe and Japan

Some facts and figures

- NN's roots lie in the 18th- century the Netherlands
- Strong business positions; market positions built organically
- Unified international culture with shared best practices
- 17 million customers (excl. NN IP)
- About 15,000 employees
- Successful IPO on 2 July 2014
- Businesses rebranded to "NN" in 2015
- ING's divestment of NN Group completed in April 2016
- Tender offer for Delta Lloyd successfully completed in April 2017
- Shareholders' equity of EUR 22.7 bn at 15 February 2018
- Credit ratings¹: A/stable (S&P), A+/stable (Fitch)

Key takeaways:

1. We are a European financial company, meaning we are regulated by the Dutch National Bank but also by other regulators
2. We have a lot of 'proven technology'
3. We are of reasonable size

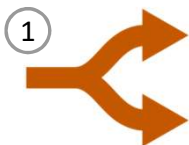


1. Financial Strength Ratings

7

7

NN IT Strategy



Split from ING

During the financial crisis, ING received financial aid from the Dutch Government.

In return, ING had to split off all high risk activities (insurance and asset management activities).

This led to a huge disentanglement program where meeting the deadline was the most important goal.



Simplify

After the split the focus shifted to lowering the IT cost drastically. This led to 4 programs:

- Anita: replatforming our mainframes to X86
- Bonita: Move our workloads from our own datacenters to public cloud
- Consuela: Optimize workplace services (e.g. move from a mail solution managed by an integrator to Microsoft Office 365)
- Doloris: Change the way of working (e.g. Agile and DevOps)



Co-driving the business

"Building technology services through speed, quality & craftsmanship to delight our customers"

Use cloud as an enabler for automation to create speed and more predictable quality & control.

Use cloud technologies to provide new possibilities to our business (e.g. new data analytics capabilities), and lower the cost.



8

8

Four Things to Know About Our Journey



Started during simplify (cost reduction program)

Original plan was to build all IT services from the service catalog on cloud (IaaS based) and redeploy all the applications on the cloud.

This was more difficult than expected. What worked on-prem did not always work on cloud.



Dual cloud strategy

Dual cloud because:

1. Azure and AWS then both had their unique strengths
2. Exit strategy, try to avoid lock in at one cloud provider



Cloud program is merged and rebooted

Merged with the Agile / Devops transformation program.

Downsized from 100+ people to 2 small core teams (20FTE).

Reset goal: Focus on cloud native solutions and automation, all to support Phase 3, co-driving the business.

- Azure focusses on data and PaaS services
- AWS focusses on IaaS based services



V-motion from own DC to IBM to AWS

Plan B to still make true on the promise to empty our data. Goal: Avoid an investment and lock in (due to depreciation)

First V2V to VMware on IBM Bluemix because of timing. When available move to VMware on AWS to support further transformation.



9

9

Key Learnings



Adjust operating model to cater for new technology



Creating the right mindset and culture



Getting or creating the right skills



10

10



Target Operating Model (TOM)

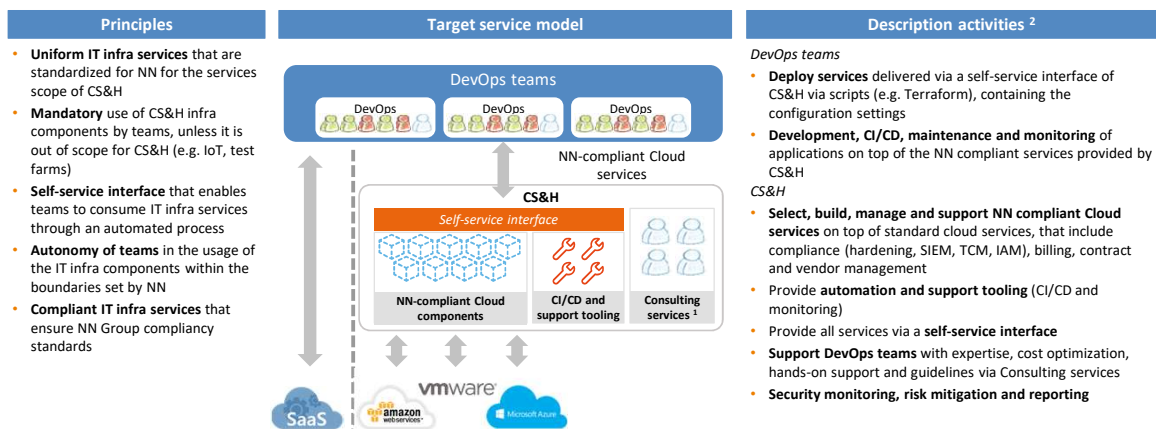


11

11

Target IT infrastructure operating model

CS&H offers NN-compliant consumable services and tooling to DevOps teams via the self-service interface



¹ Consulting services provide guidelines, support and expertise for design and development of infra capabilities

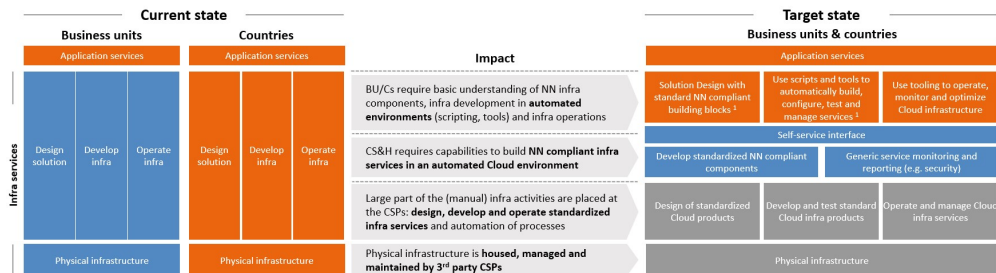
² A concept capability model is being developed, that includes detailed responsibilities and activities (e.g. ITIL) for the application teams and CS&H

12

12

Tasks and Responsibilities

The target operating model requires new skills and capabilities within CS&H and in the business teams



Description

- Business Units and countries will extend their work with (1) design applications with standardized NN compliant infra components, (2) use scripts and automated processes to develop the infra services, and (3) apply available tooling to monitor and optimize the infra services in the Cloud
- A large part of the conventional IT activities (build, deploy, run) that is now being executed by CS&H will disappear into the Cloud via automated processes. Remaining task for CS&H is to develop and maintain standard NN compliant building blocks on top of standard Cloud products and manage the CS&H Cloud service catalogue
- A large part of the current (manual) work will move to the Cloud provider, that will create the standard Cloud infra services that can instantly be deployed by NN
- Physical infrastructure will no longer be on-premise and will be managed by the Cloud Service Provider in the Cloud

BU/Country CS&H Cloud service provider

¹ Design and development supported by consulting services



13

13



Security and Compliance



14

14

General Adopted Security Approach

Framework for cloud risk control – based on ISF Framework

Step 1: Perform a risk assessment.

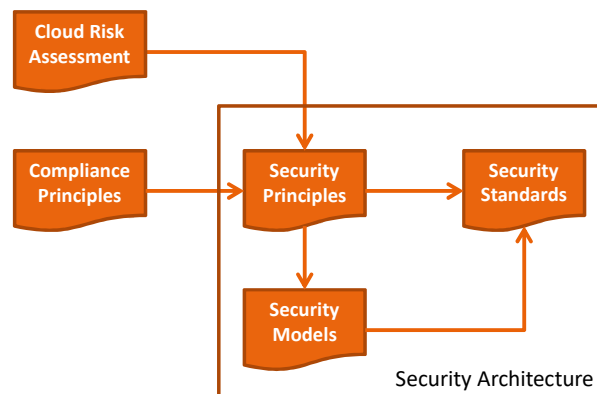
Step 2: Set boundaries with a set of compliance principles.

Step 3: Determine a list of security principles

The security principles are meant to mitigate the risks found during the cloud risk assessment. The security principles should be checked against the compliance principles.

This cloud risk and security framework is sent to the regulators.

Step 4: Let the cloud teams build services compliant with the cloud risk and security framework.



15

Cloud Security & Risk Framework

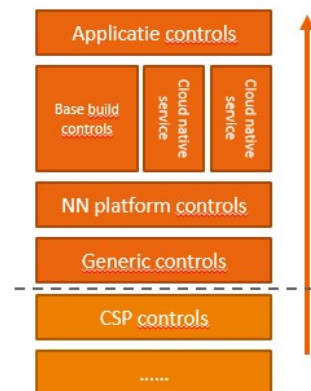
• Last version of this NN framework

- Cloud Security and Risk Framework – version 2.1 – November 2018
- ISF Framework

• How are measures and principles required by this framework implemented

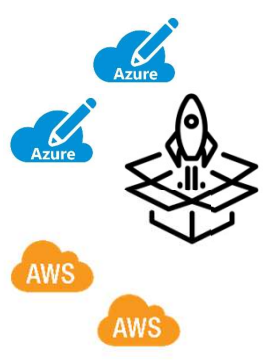
- AWS key controls defined on platform and product (i.e. S3) level
- Application controls are described in the Operational Security Guideline of the application
- Only identified traffic is allowed over this connection
- All communications are encrypted with SSL
- System administration by NN Group, Functional Management by NN Business Unit
- NN Active Directory authentication, MFA for system administration and Role Based Access
- Security Event Monitoring infrastructure is operated and maintained by dedicated team

• Non compliances if any




16

16




The Azure & AWS Platform




17

17

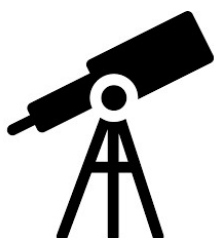
Cloud Adoption Acceleration





18

18



The Cloud Vision 2019

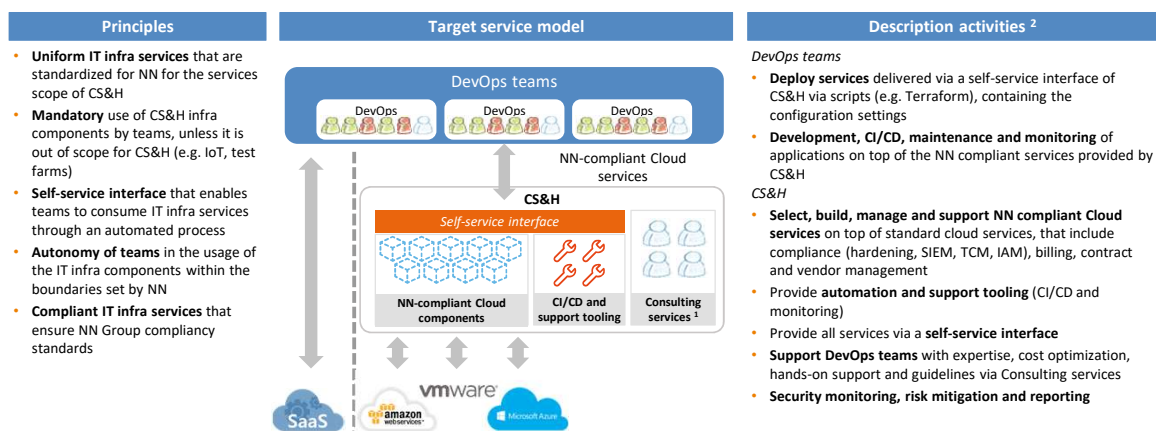


19

19

Target IT infrastructure operating model

CS&H offers NN-compliant consumable services and tooling to DevOps teams via the self-service interface

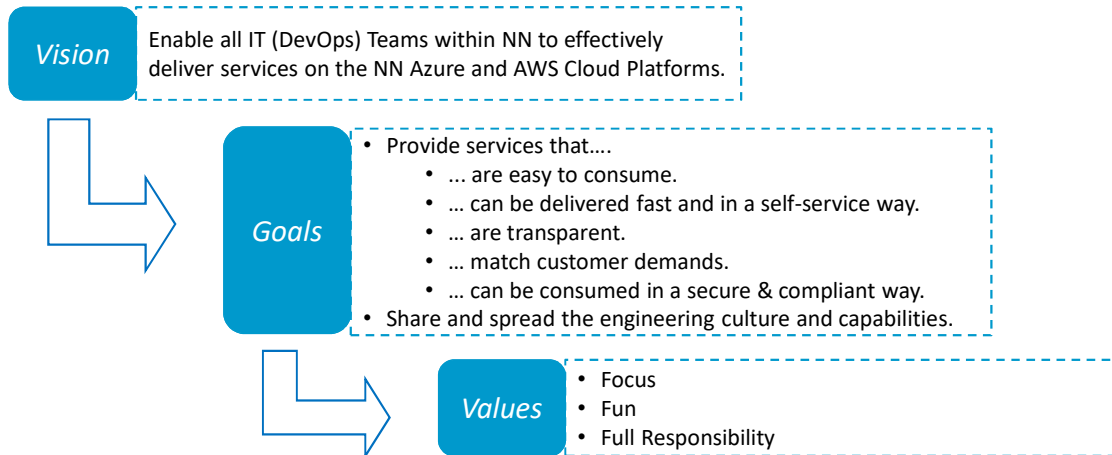


¹ Consulting services provide guidelines, support and expertise for design and development of infra capabilities

² A concept capability model is being developed, that includes detailed responsibilities and activities (e.g. ITIL) for the application teams and CS&H

20

NN Cloud Vision 2019



21



Security & Compliance
Balance between Freedom and Control



22

22

What is the Right Balance Between Freedom and Control?

- Risk assessment - biggest risks are known.
- Different internal customers with different requirements, need certain level of freedom.

Public Cloud is not Secure nor Compliant by default, you must do it yourself.

- Balance between freedom and control:
 - Main guardrails centrally implemented (Enforced vs. Monitored).
 - Boundaries to minimize blast radius.

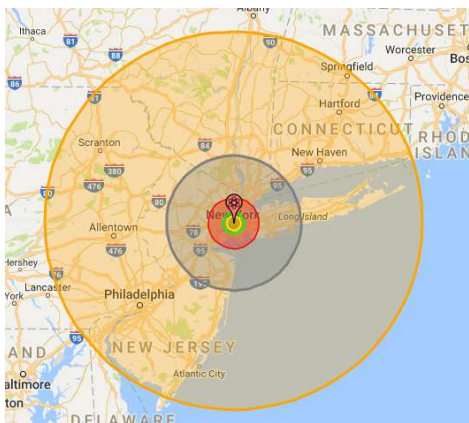


23

23

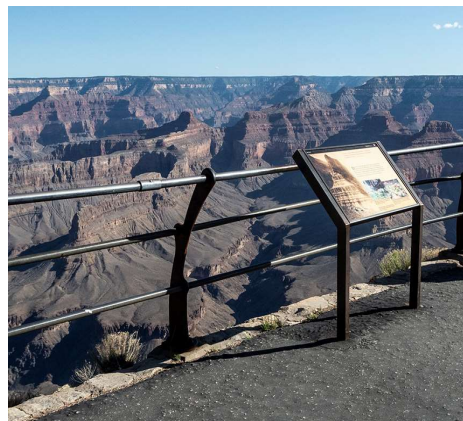
Boundaries

Minimize the impact in case of an incident /



Guardrails

Prevent and monitor the (main) risks

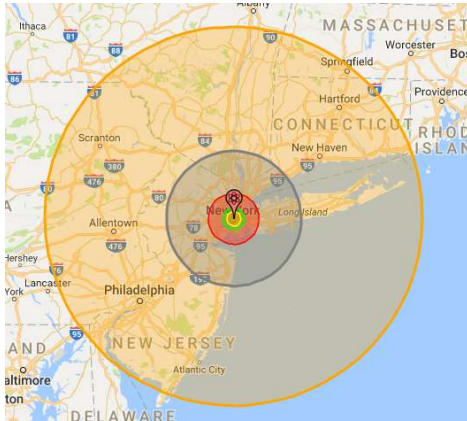


24

24

Boundaries

Minimize the impact in case of an incident /



Guardrails

Prevent and monitor the (main) risks



25

25



26

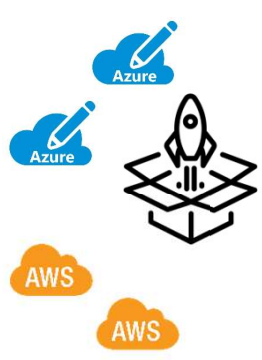
26




27



28



The Managed Subscription & Account Model

 29


29

Multi-Subscription/-Account Setup

What kind of characteristics do we need?

Unmanaged/Sandbox	Engineering	Standard/Production
<p><i>Experiment in a completely independent and ungoverned setup.</i></p> <ul style="list-style-type: none"> Experiment with Azure and AWS in a completely independent setup. Full freedom and control for the owner of the Subscription or Account. No compliance is enforced. No NN network connectivity. Not AD integrated. Just profit from the NN-Group Azure or AWS discounts and nothing more. Most important rule: No NN data is allowed in a Sandbox environment. 	<p><i>Experiment with Azure/AWS capabilities here.</i></p> <ul style="list-style-type: none"> Develop new and existing Service Catalogue items. Limited policy set is enforced to prevent most dangerous actions. Full Production policy set is monitored. Freedom to add new policies (enforced or monitor) to the Subscription or Resource Groups. No network connectivity to on-premises. 	<p><i>Run your DTAP workloads here.</i></p> <ul style="list-style-type: none"> Consume NN compliant service via a Service Catalogue. Consume non-compliant non-Service Catalogue items at own risk. Production policy set is enforced to prevent dangerous actions. Production policies monitored, to provide insight in possible risks. Benefit from cost saving policies. Implement additional compliance measures and policies on your own behalf. Connection to on-prem and other spokes available.

"With Great Freedom Comes Great Responsibility"

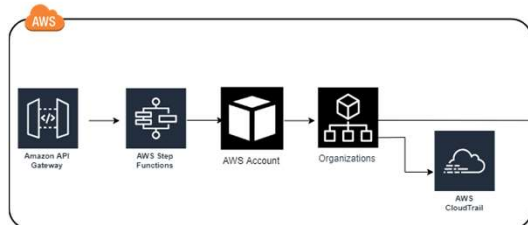
 30

30

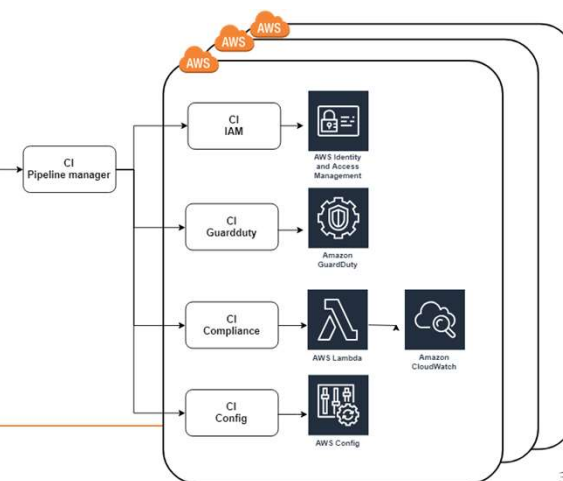
Multi-Subscription/-Account Setup

Deployment model – AWS example

1. Infra as code
2. Automatically tested



3. Automatically deployed in all accounts
4. Results sent to the central AWS team

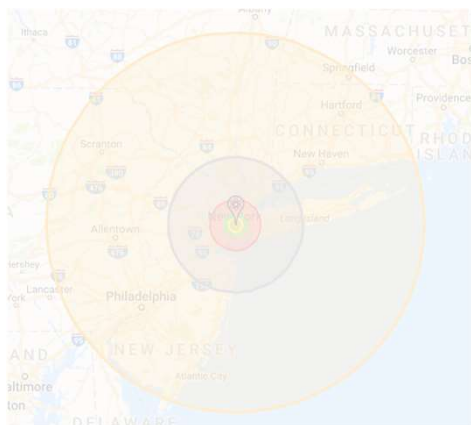


31

31

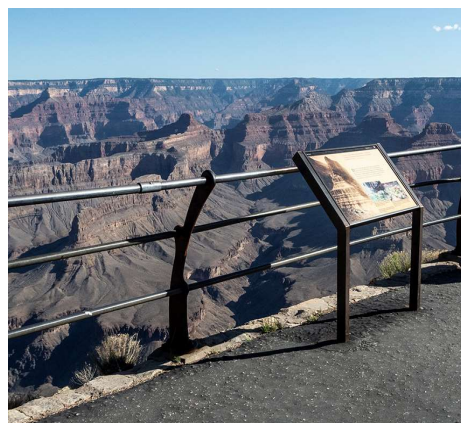
Boundaries

Minimize the impact in case of an incident /



Guardrails

Prevent and monitor the (main) risks



32

32

Security & Compliance Measures (1)

How we balance between freedom and control

Goal: Providing a secure and compliant Azure and AWS platform to our customers.

IAM

- Integration with the NN Active Directory services.
- SSO with multi-factor authentication.

Change control and traceability

- No manual access to Acceptance/Production Accounts.
- In case needed, only peer-reviewed JIT access.
- Everything is automatically tested and deployed via a pipeline.
- Use of Azure DevOps to track changes back to user-stories.

Security Information and Event Management (SIEM)

- Benefit as much as possible from the Azure or AWS platform native intelligent tooling (e.g. LogAnalytics / Event Hub and Security Center).
- Relevant logging centrally collected and forwarded to the NN SOC – for NN Group level monitoring. They inform the central team or take mitigating action if needed.



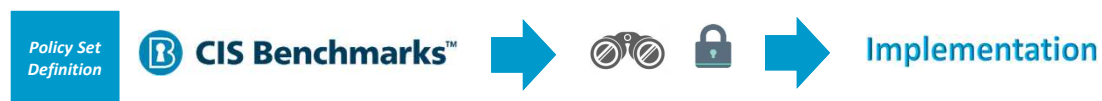
33

33

Security & Compliance Measures (2)

How we balance between freedom and control

Technical State Compliance Monitoring (TSCM) via Policies



Lessons learned:

- Started manually, but lack of traceability and a lot of work → automate!
- Adopt market standards.
- When you make compliance easy, adoption and use will come all by itself.

Remember: You're not the first organization with additional compliance requirements!



34

Azure Policies

Priority of CIS Benchmark Items

Policy Overview

Coverage High Priority CIS Benchmark Items

Coverage Medium Priority CIS Benchmark Items

Coverage Low Priority CIS Benchmark Items

NN Policy

CIS Policy

Risk	Description	Rationale	Impact	Profile Applicability	Status	Assess Baseline Policies	NN Azure Policies
2.1 Apply tag and its default value		Keys cannot be used beyond their assigned expiry times respectively. This would cause you to lose permanently as if places they are used.		Level 2	Not Monitored		\$11e6110-10-a9f-480a-b05d-555555555555
2.2 Enforce CostCenter tag and its value		Tags cannot be used beyond their assigned expiry times respectively. This would cause you to lose permanently as if places they are used.		Level 2	Not Monitored		\$11e6110-10-a9f-480a-b05d-555555555555
2.3 Ensure related user benefits is enabled on Virtual Machines			None	Level 2	Not Monitored		

Risk	Description	Rationale	Impact	Profile Applicability	Status	Assess Baseline Policies	NN Azure Policies
4.1.1 Enable auditing		The Azure platform allows you to create a SQL server as a serverless, auditing auditing at the server level ensures that all existing and newly created databases on the SQL server remain in a compliant state.		Level 1	Enforced		\$11e6110-10-a9f-480a-b05d-555555555555

A presentation slide with a white background. On the left side, there is a black outline icon of a lightbulb. To the right of the lightbulb is a solid blue rectangular box containing the text 'Key Takeaways' in a white, italicized, sans-serif font. At the bottom left of the slide, there is a logo consisting of a stylized orange 'N' inside a circle, followed by the letters 'NN' in a bold, black, sans-serif font. A thin orange horizontal line is positioned above the logo. In the bottom right corner, the number '36' is displayed in a small, black, sans-serif font.

Key Takeaways

- Don't copy the way you do IT on-premise to Cloud.

If you want to benefit from cloud you have to do IT, and therefore also security and compliance, in a different way (people, process and technology).



- Think carefully about the risks - balance freedom and control.

We advise the central IT team to focus on mitigation by means of boundaries and guardrails, with a balance between freedom and control that fits your company and risk appetite. Allow for sufficient freedom to capture the benefits of cloud technologies.



- Automate! To be able to scale and control the environment.



37

37

Our Next Steps

- Expand the use of the Azure and AWS platforms within NN.
- Increase the level of insight and (automated) remediation on security and compliance. Provide aggregated compliancy insights across cloud resources.
- Rethink our current scaling capabilities – this will work for 500 accounts, but will it also work for 1500?
- Increase the level of knowledge and skills regarding usage of the cloud platforms.
- Improve the use and way of enabling a community model within the organization, enable the developer community to create re-usable compliant building blocks.



38

38

Balance Between Freedom and Control



39

39



40