ALT

nexxbiz

— CRUISING AT 70,000 FT

FROM POLICY TO PROOF

How insurers turn trust, suppliers and software into evidence-based confidence.

One descent: from the insurance promise to practical proof.

70,000 FT

ALT

70,000 FT

nexxbiz

70,000 FT · WHY THIS PERSPECTIVE

We operate inside the insurance promise.

Nexxbiz

Active in the insurance market since 2003, delivering a policy administration platform for insurers.

Our customers

Example Dutch customers include Monuta, DELA, NH1816 and Figo Pet.

My lens

Shamin Hameed — 20+ years in the IT industry. Over the last 12 months, helping our customers implement the DORA chain across risk, controls, suppliers and evidence.

nexxbiz.io

ALT

nexxbiz

— 70,000 FT · THE STORY MAP

Before we descend, here is how the story will evolve.

70,000 FT
The promise
Insurance starts as trust.

60,000 FT
The sector view
DORA, DNB, standards and reports.

45,000 FT
The governance layer
Risk, suppliers, controls and evidence.

30,000 FT
The continuity lens
Scenarios, recovery and validation.

10,000 FT
The AI shift
Policies become guardrails.

0 FT
The landing
One service. One scenario. One proof pack.

Context first, content second — then action.

70,000 FT

ALT

65,000 FT

nexxbiz

65,000 FT · WHY INSURANCE EXISTS

Insurance is a promise made before the bad day arrives.

Policy sold		Moment of truth
calm day · expectation set	PROMISE →	claim · loss · disruption

> A policy is written in legal language. The promise is executed in software.

The promise is the product.

ALT

nexxbiz

65,000 FT · THE PROMISE CHAIN

That promise now runs through people your customer will never meet.

Policyholder → Insurer → PAS / SaaS → Cloud → Identity → Data → Support → Subcontractors

A failure three vendors down is still a trust problem at the front door.

65,000 FT

ALT

nexxbiz

60,000 FT · SHARED RESPONSIBILITY

We all share responsibility for the promise.

EXECUTIVE
Accepts risk
Sets appetite and decides under pressure.

TECHNOLOGY
Designs recovery
Builds resilience, validation and clean operations.

PRODUCT / OPS
Protects the flow
Owns workflows, data quality and daily continuity.

COMMERCIAL
Translates proof
Turns evidence into customer confidence.

Compliance is not a department. The whole organization creates the proof.

60,000 FT

ALT

nexxbiz

60,000 FT · REGULATOR VIEW

Not “DORA is implemented.” Prove DORA works.

DORA

Operational resilience

Can you withstand, respond and recover from ICT disruption?

CHAIN

Third-party dependency

Critical ICT suppliers and outsourcing are part of the risk picture.

EXPECTATION

Make it practical

Controls, tests, evidence and decision rights must work in real life.

> **The shift is from documented intention to demonstrated operational resilience.**

Can the sector prove it keeps functioning when IT fails?

60,000 FT

ALT

55,000 FT

nexxbiz

55,000 FT · TWO TRUST PROMISES

Two things make the software promise credible.

Data integrity
Is the policy, premium, claim and customer data complete, accurate and usable?

AND

Service continuity
Can the service keep running, recover, validate and return safely?

> **Availability without trustworthy data is noise. Data integrity without service continuity is a promise nobody can access.**

ALT

nexxbiz

55,000 FT · WHERE CERTIFICATIONS FIT

Certifications are useful. They are not the operating model.

START HERE

Governance model + risk model

Standards and reports are proof points around it — not a replacement for it.

ISO 27001

ISO 22301

ISO 9001

ISAE 3402

A certificate gets you into the conversation. Evidence keeps you trusted.

55,000 FT

ALT

nexxbiz

50,000 FT · CERTIFICATION VS ASSURANCE REPORT

Snapshot vs operating period.

Certification

A momentary check: “were we compliant at this point?”

VS

Assurance report

A period of operation: “did controls work over time?”

> **Assurance = confidence based on evidence.**

50,000 FT

nexxbiz

— 50,000 FT · THE SUPPLIER REPORT MOMENT

Your supplier sends the report. Now what?

Supplier evidence
Certificate, assurance report, test result or audit response.

→

Three questions
- Scope?
- Evidence?
- Gap?

→

Your conclusion
What risk remains with us, and who accepts it?

Supplier evidence is input. Your risk decision is the output.

ALT

nexxbiz

45,000 FT · OUTSOURCING

Execution moves out. Accountability stays in.

RISK APPETITE · REGULATION · CUSTOMER PROMISE

Insurer

Owns customer impact, regulatory conclusion, risk appetite and residual risk acceptance.

Supplier chain

Performs part of the service: PAS, SaaS, cloud, subcontractors, monitoring, recovery and evidence.

Critical outsourcing does not move work outside the risk boundary.
It changes who executes — not who is accountable.

True partnership avoids overhead: match supplier evidence to customer risk, then close the gaps together.

45,000 FT

ALT

nexxbiz

45,000 FT · CRITICAL OUTSOURCING PARTNERSHIP

Choose the partner who can prove the controls, not just show the badge.

Insurer risk lens

The insurer owns the customer promise, regulatory conclusion and residual risk.

risk appetite · customer impact · DORA chain

Shared control map

True partnership starts when customer risk and supplier controls are mapped to one operating picture.

scope · evidence · exceptions · gap closure

Supplier proof lens

The supplier proves which controls operated, where the report scope ends and which gaps remain.

ISAE 3402 · tested controls · period evidence

Certification

Useful baseline: a management system was assessed.

BETTER FOR CRITICAL OUTSOURCING →

ISAE 3402 report

More useful for outsourcing: scoped controls, operating evidence and exceptions over a period.

The right partner reduces overhead by making evidence usable, comparable and mapped to the risk you actually own.

45,000 FT

ALT

nexxbiz

— 40,000 FT · COMPLIANCE'S REPUTATION PROBLEM

Compliance fails when it describes paperwork instead of work.

A wall
Annual panic, screenshots, copied policies and CISO-only ownership.

VS

A guardrail
Clear owners, everyday evidence, design-time controls and faster decisions.

A good governance model lets the business move safely.

40,000 FT

ALT

nexxbiz

35,000 FT · SERVICE CONTINUITY

Service continuity is not one big thing. Break it apart.

~~BUSINESS CONTINUITY~~

Scenario | Impact | Owner | Runbook | Evidence | Improvement

Continuity is a chain of decisions that must work under pressure.

35,000 FT

ALT

30,000 FT

nexxbiz

30,000 FT · PICK A SCENARIO

Five failure modes worth testing before they test you.

NEXXBIZ BC TESTING FRAMEWORK

- Isolated component failure
- Cascading failure
- Site-level failure
- Malicious incident
- Cloud region failure

From the Nexxbiz Business Continuity Testing framework — scenarios that help start the thinking process.

ALT

nexxbiz

25,000 FT · RECOVERY MEANS MORE THAN SERVERS

Recovered is not the same as safe to trust again.

Infrastructure	Data	Functional	Process	Supplier	Restore

> A restored platform with questionable data is not restored.

25,000 FT

ALT

nexxbiz

20,000 FT · SHIFT LEFT

Design continuity before the incident asks for it.

BOLTED ON LATE

- After go-live
- Under audit pressure
- Owned by no one clearly
- Tested rarely

DESIGNED IN EARLY

- During architecture review
- Before supplier sign-off
- Control owner assigned
- Evidence generated as work happens

NEXXBIZ PRACTICE LENS · SHIFT LEFT

You do not buy insurance after the house has burned down.

20,000
FT

ALT

nexxbiz

15,000 FT · THE MORNING TEST

Tomorrow, call someone and say: “We have been hacked.”

Then watch the next ten minutes. It tells you more than any policy binder.

- Who is called first?
- Where is the runbook?
- Who calls the supplier?
- Who can engage responders?
- Who calls cyber insurance?
- Who speaks to customers?
- Who informs the regulator?
- Who keeps the evidence log?

A runbook is not a document. A runbook is rehearsed behaviour.

15,000 FT

nexxbiz

— 15,000 FT · TWO DIFFERENT JOBS

Declaring a disaster and recovering from one are not the same job.

CRISIS AUTHORITY

“Do we declare disaster mode?”

Owns business, legal, regulatory, financial and reputational impact.

RECOVERY LEAD

“How do we restore safely?”

Coordinates technical and operational recovery.

EVIDENCE OWNER

“Can we prove what happened?”

Owns timeline, decisions, validation and lessons learned.

A disaster is declared by accountability, not by technology.

ALT

nexxbiz

— 10,000 FT · THE NEXT READER

Your next policy reader might not be a person.

AI agents will increasingly write code, generate configuration, choose packages, update documentation, trigger workflows and prepare evidence.

> **If an AI agent downloads a package or changes a configuration, how does it know which policy it must follow?**

Agentic AI does not create new governance gaps. It makes the old ones visible.

10,000 FT

nexxbiz

ALT

5,000 FT · WHAT THIS MEANS FOR NEXXBIZ

Our learning after 12 months of incorporating AI: governance must become a live blueprint.

TEKLARO

A live blueprint for people and AI

Policies, controls, owners, suppliers, risks, certifications and evidence in one operating view.

INPUT
Standards & reports
What must be true.

STRUCTURE
Controls & owners
Who makes it true.

OUTCOME
Live evidence
How people and AI can act on it.

Continuous compliance has always been the dream. AI makes the dream urgent.

5,000 FT

ALT

nexxbiz

0 FT · MONDAY MORNING

Do not try to solve everything tomorrow. Build the blocks.

01	02	03	04	05
Pick one service	**Map the chain**	**Ask for proof**	**Test a scenario**	**Create proof pack**
PAS is a strong place to start.	Insurer · SaaS · cloud · data · support.	Scope, evidence, gap, residual risk.	One realistic failure mode.	Owners, evidence, gaps, actions.

> **Start with one service, one scenario, one supplier and one proof pack. Then scale.**

0
FT

— óó TAXI · STEAL THESE LINES

Next time you sit in a meeting, remember these lines.

CEO / DIRECTOR

óó

You can outsource execution, but not accountability.

NON-EXECUTIVE DIRECTOR

óó

The board must know whether the promise can survive stress.

CTO / IT LEAD

óó

Resilience is not proven by architecture diagrams.

PRODUCT MANAGER

óó

Data integrity is a product promise, not only a technical control.

ACCOUNT MANAGER

óó

A certificate opens the conversation; evidence wins the trust conversation.

RISK / COMPLIANCE

óó

Compliance should describe how the organization actually works.

FLIGHT LOG · SOURCES & CREDIT

What this deck stands on.

Nexxbiz
Logo and public company context used for the speaker lens.
nexxbiz.io

EIOPA
DORA overview and DORA oversight material.
eiopa.europa.eu

DNB
DORA/open-book supervision and outsourcing expectations.
dnb.nl

ISO
ISO 27001, ISO 22301 and ISO 9001 management-system framing.
iso.org

IAASB
ISAE 3402: Assurance Reports on Controls at a Service Organization.
iaasb.org

Nexxbiz
Business Continuity Testing framework: scenarios and assurance areas.

Use this slide as backup. The live close can stop on the role-based quotes.