NEXUS 7
RISK ASSESSMENT

From Vulnerability to Strength

Transform Cybersecurity Behavior with NEXUS-7

An evidence-based approach to the human factor in cybersecurityRetry

Executive Summary

In an era where technology is increasingly well-protected, **human behavior remains the determining factor** for cybersecurity. A single click on a phishing email, the disregarding of rules, or careless handling of confidential information can create serious risks – despite multimillion investments in technical security.

NEXUS-7 helps organizations transform cybersecurity from a vulnerability into a strength by making employee behavior transparent and proactively influencing it. Our validated, scientifically grounded approach makes the difference between responding to incidents and structurally preventing them.

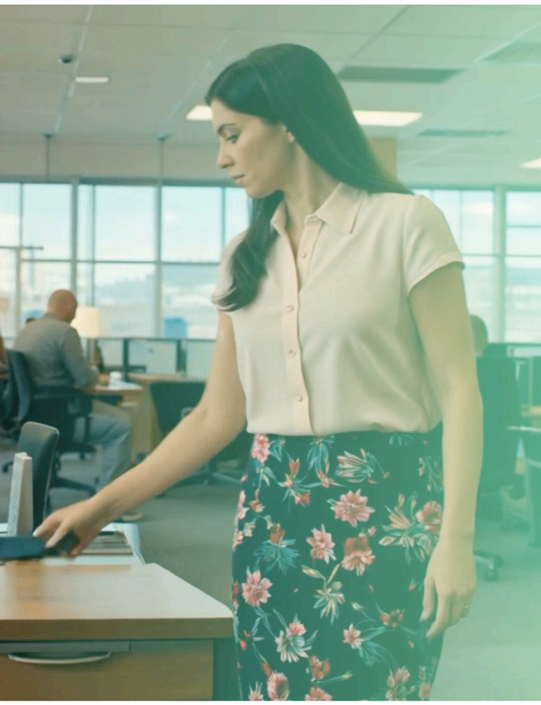
Direct Measurable Results

✅ **Fewer cyber incidents** through conscious, secure behavior
✅ **Self-directed employees** who act safely
✅ **Continuous improvement** process with measurable progress
✅ **Data-driven policy** for targeted measures

What NEXUS-7 Offers Your Organization

Evidence-based behavioral analysis that makes risks measurable and visible:

- **Identify red flags** in behavior at an early stage
- **Structured development cycle** for sustainable behavioral change
- Individual and organizational **insights** for targeted actions
- **Continuous improvement** cycle, not a one-off training session



The Point of Improvement: The Human Factor

Why Technology Alone Isn't Enough

Cybersecurity problems threaten not only data and systems, but also the **financial stability, business continuity, trust and strategic positions of organizations**. Whilst organizations invest billions annually in technical security measures, human behavior remains the weakest link.

The Hard Facts:

- 95% of all cyber incidents are caused by human error
- An average data breach costs Dutch organizations €3.9 million
- 60% of affected companies lose customers following an incident
- Traditional awareness training has only 15-20% lasting effect

The Challenge: Deep-rooted Behavioral Patterns

Employees often display **deep-rooted behavioral patterns** that bring both opportunities and risks:

Behavioral Pattern	Positive Effect	Cybersecurity Risk
Impulsivity	Quick thinking, problem-solving	Clicking without thinking, phishing
Perfectionism	Precise, detail-oriented	Avoidance of new systems
Rule rejection	Creative, innovative	Circumventing security protocols
Stress sensitivity	Empathetic, engaged	Errors under pressure, social manipulation
Conflict avoidance	Harmony, team player	Not reporting incidents

NEXUS7
RISK ASSESSMENT

These patterns can have positive effects, such as resilience and stress resistance, but also negative consequences for cybersecurity behavior.

Recognizing 'red flags' in cybersecurity behavior is a crucial first step toward change.

What Current Solutions Are Missing

Traditional cybersecurity training fails because it:

- ❌ Is one-off, without follow-up or repetition
- ❌ Is generic, not tailored to individual behavior
- ❌ Transfers knowledge but doesn't achieve behavioral change
- ❌ Doesn't measure the effect on actual behavior
- ❌ Provides no insight into underlying drivers

The Solution: NEXUS-7 Security Behavioral Analysis

NEXUS-7 offers a **structured, scientifically grounded solution** to detect, analyze, and sustainably change cyber(in)secure behavior.

Our Security Behavioral Analysis provides **visibility, insight, detection, warning, and protection** against cyber threats by monitoring deviant behavior and providing input for behavioral change.

Three Pillars of the NEXUS-7 Approach

1. **Insight into Behavior**

   Scientifically grounded insight into how employees handle cybersecurity. In just 18 minutes, you receive:

   - An individual behavioral profile across 7 critical levels
   - Analysis of 11 specific impact areas
   - Identification of personal red flags
   - Comparison with organizational benchmark

2. **Input for Action**

   Concrete tools to influence behavior in a targeted way:

   - Personalized recommendations per employee
   - Management dashboards for teams and departments
   - Prioritization of interventions based on risk
   - Practical tips and action points for immediate use

3. **GROW! - Sustainable Behavioral Change**

   Structural development toward lasting secure behavior:

   - Continuous feedback loop via repeated measurements
   - Self-directed employees who monitor their own behavior
   - Training and coaching tailored to personal profile
   - Measurable progress over time

Het NEXUS-7 platform: Intelligence meets usability

Our cybersecurity behavioral approach combines an advanced SaaS solution (Software as a Service), developed by Roger Heykoop, with scientific depth, created by Nina Binnendijk, and ease of use:

For Employees

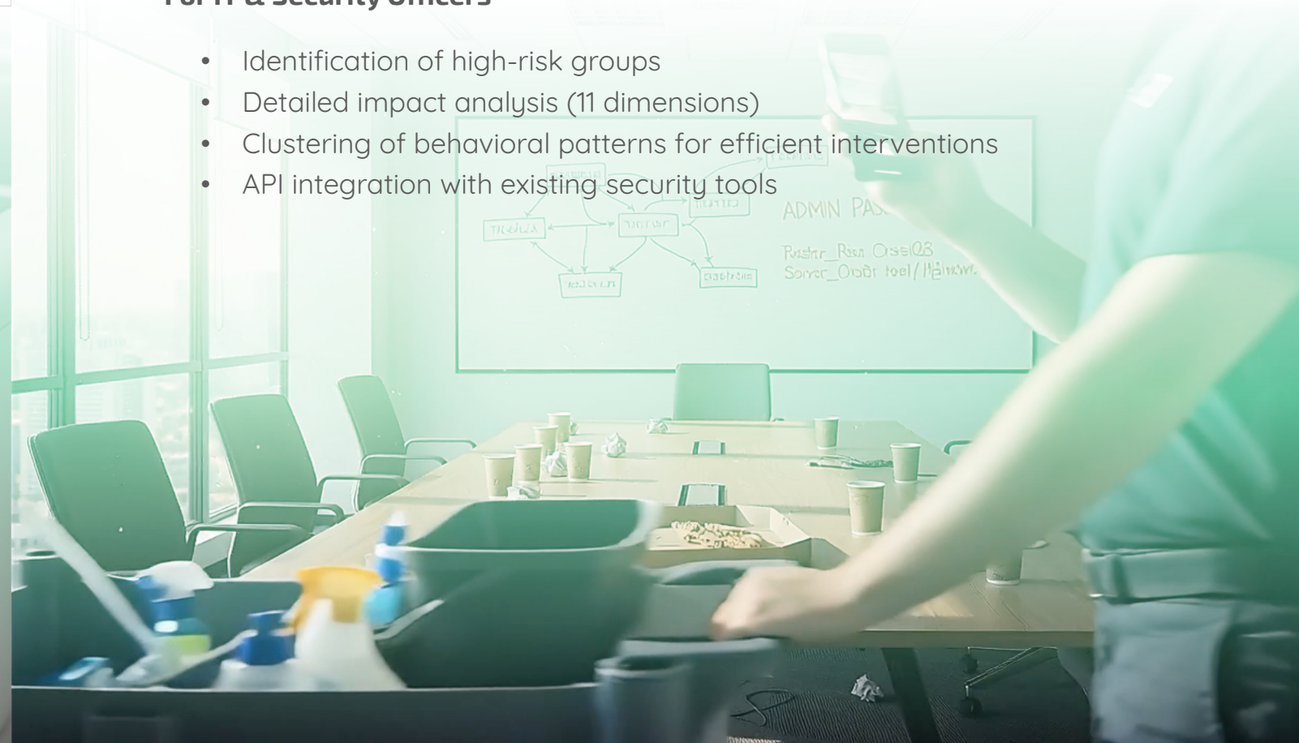
- **Q-sort assessment** in 18 minutes via intuitive drag-and-drop interface
- Personal report with positively framed insights
- Bilingual support (Dutch/English)
- Mobile-friendly, accessible from any device

For HR & Management

- **Real-time dashboards** with organizational overview
- Exportable reports (PDF, Excel, CSV)
- Benchmark comparisons between teams and departments
- Trend analysis for long-term monitoring
- AI-generated recommendations per cluster

For IT & Security Officers

- Identification of high-risk groups
- Detailed impact analysis (11 dimensions)
- Clustering of behavioral patterns for efficient interventions
- API integration with existing security tools

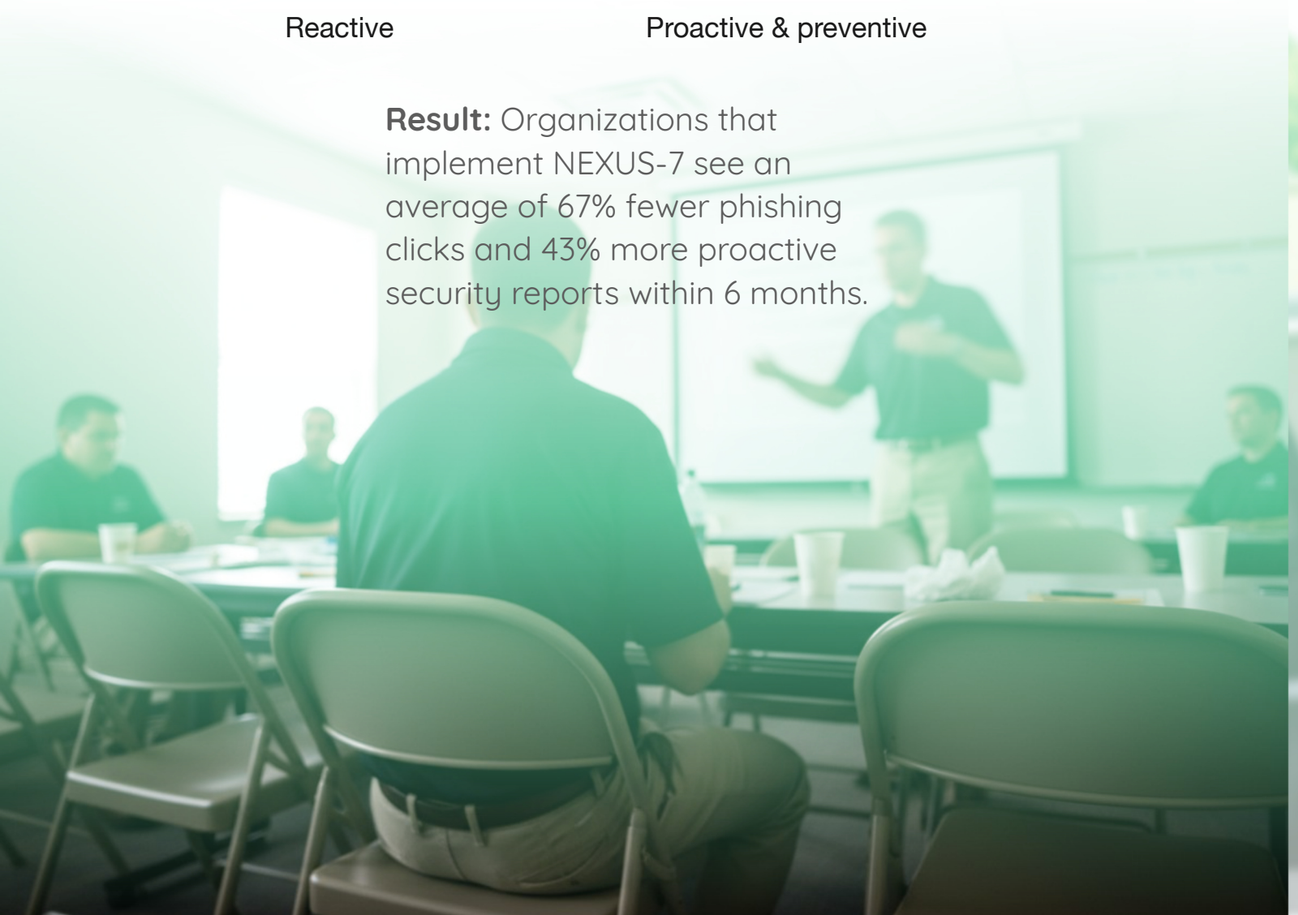


The Power of Data-Driven Behavioral Change

NEXUS-7 goes beyond traditional awareness:

Traditional Training	NEXUS-7 Behavioral Analysis
One-time event	Continuous cycle
Generic content	Personalized insights
Knowledge transfer	Behavioral change
No measurement	Objective data
Compliance-oriented	Development-oriented
Reactive	Proactive & preventive

Result: Organizations that implement NEXUS-7 see an average of 67% fewer phishing clicks and 43% more proactive security reports within 6 months.



NEXUS7
RISK ASSESSMENT

Scientific Foundation: The Q-Methodology

Validated Research Technique

The NEXUS-7 Security Behavioral Analysis is based on the **validated Q-methodology,** a scientific research technique developed by:

- **Prof. Dr. W. Stephenson** (1902-1989): Founder of Q-methodology
- **Prof. Dr. S. Brown** (1980: Political Subjectivity): Theoretical elaboration
- **Prof. Dr. M. Brouwer** (1929-2001): Dutch implementation with Drs. C.T.M. Binnendijk: From 2001: Academic and commercial (Q-Research, EnSemper). Founder Nexus-7.

This methodology, with roots in psychology and physics, has proven itself worldwide in diverse research fields including behavioral psychology, organizational development, and risk management.

Why Q-Methodology Is Unique

What makes the NEXUS-7 Security Behavioral Analysis unique is that candidates are challenged to create a ranking of 42 cybersecurity statements (indicating priorities) within a structured grid.

The Power of Forced Choices

This forces them to weigh **each statement** against all others, which amounts to at least **420 implicit choices** per candidate. Through this intensive weighing process, **a detailed, nuanced insight** (personal profile) emerges into individual behavioral preferences in cybersecurity contexts.

Why This Works:

- People cannot mark all statements as "important"
- Forced prioritization reveals true values
- Implicit choices are harder to manipulate
- Result is much richer than Likert-scale questionnaires

From Data to Insight

The 42 statements are carefully distributed across:

- **7 levels (drivers)** of the NEXUS-7 Development Cycle (6 statements per level)
- **11 impacts** that influence cybersecurity behavior (3-4 statements per impact)
- **Perfect balance** between positively and negatively framed statements (21/21)

This scientific distribution ensures valid, reliable measurements that are repeatable and comparable.

The NEXUS-7 Development Cycle

Seven Drivers for Behavioral Change

The cybersecurity statements in the Security Behavioral Analysis are carefully distributed across the **seven drivers (levels) of the NEXUS-7 Development Cycle.**

This model, based on the **Linguistic Programming Model** (Prof. Dr. G. Bateson, 1904-1980; R. Dilts, NLP), describes seven hierarchical levels that influence behavioral change.

It functions as an analysis, change, self-regulation, training, and coaching model that helps candidates gain insight into their personal drivers toward mission-oriented, secure security behavior.

1. Environment (Context)

The physical and digital context in which employees operate.

- **Examples:** Workplace, systems, tools, procedures
- **Interventions**: Technical facilities, process optimization

2. Behavior (Actions)

The visible actions and choices employees make.

- **Examples:** Password behavior, email checking, reporting incidents
- **Interventions:** Behavioral training, simulations, feedback

3. Capabilities (Skills)

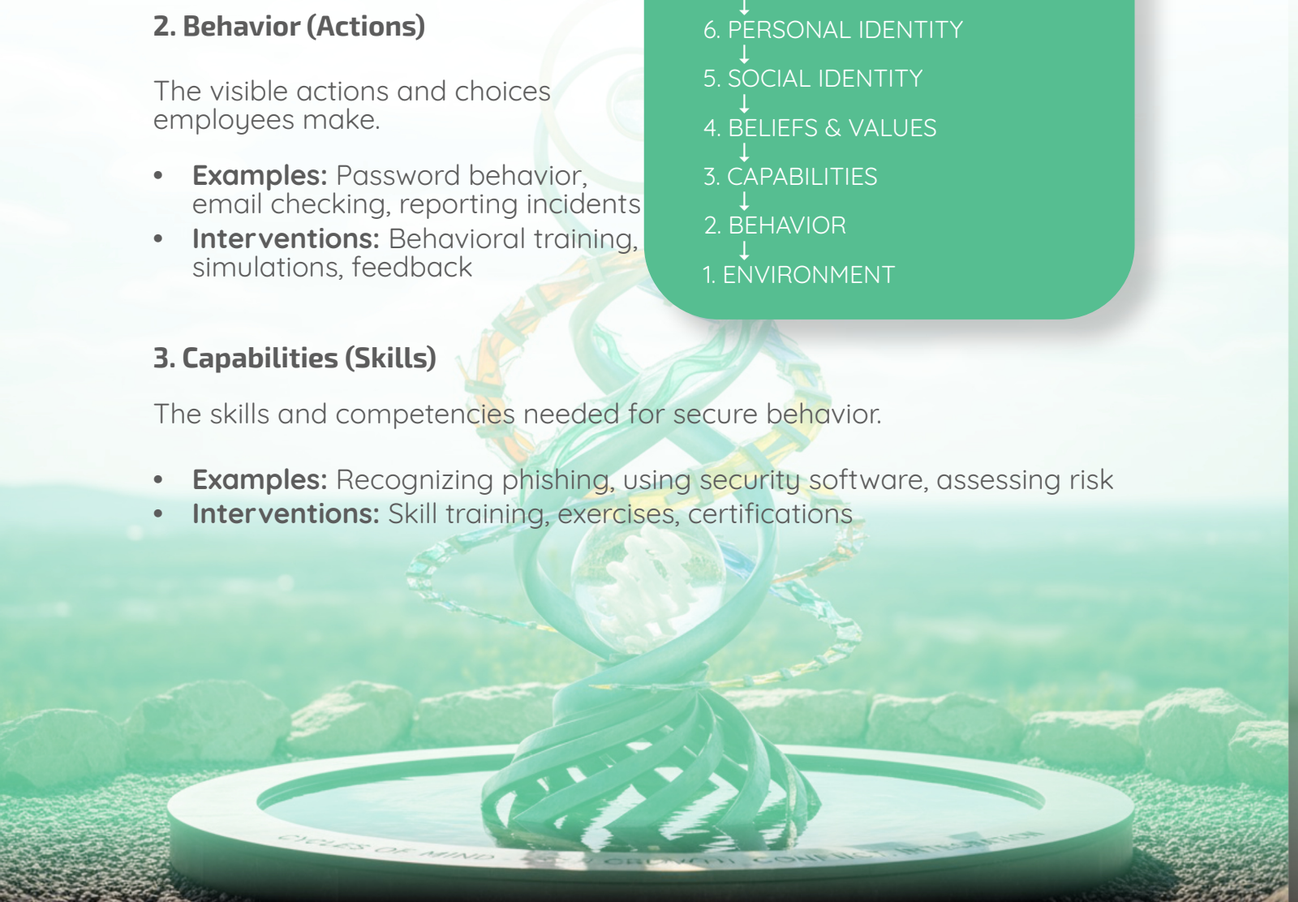
The skills and competencies needed for secure behavior.

- **Examples:** Recognizing phishing, using security software, assessing risk
- **Interventions:** Skill training, exercises, certifications

The Hierarchical Structure

Each successive driver in the cycle builds upon the previous one, whereby behavior can be systematically developed and strengthened:

7. MISSION & VISION
↓
6. PERSONAL IDENTITY
↓
5. SOCIAL IDENTITY
↓
4. BELIEFS & VALUES
↓
3. CAPABILITIES
↓
2. BEHAVIOR
↓
1. ENVIRONMENT



NEXUS7
RISK ASSESSMENT

4. Beliefs & Values (Mindset)

The deeper beliefs that drive behavior.

- **Examples:** "Security is important," "I am responsible," "Reporting is normal"
- **Interventions:** Mindset coaching, culture change, storytelling

5. Social Identity (Self-image within a group)

How employees view cybersecurity from the group perspective (teams, departments).

- **Examples:** "If the rest of the team says this procedure is safe, I just follow it," "I don't ask questions about the new security rules, everyone's already following them anyway"
- **Interventions:** Workshops on giving feedback and asking questions, role-playing where people say "no" or present divergent ideas. Coaching.

6. Personal Identity (Self-image)

How employees see themselves in relation to cybersecurity.

- **Examples:** "I am a security-conscious professional," "I am a role model"
- **Interventions:** Identity coaching, ambassador programs

7. Mission & Vision (Purpose)

The higher purpose that cybersecurity serves.

- **Examples:** Protecting customers, contributing to society, organizational goals
- **Interventions:** Purpose alignment, leadership, strategy

Continuous Improvement

The Development Cycle makes visible how **concrete steps** lead to **behavioral change**. Each successive driver in the cycle helps candidates take a step further in their development toward cybersecurity behavior, whereby the process of behavioral adjustment is **systematically and measurably supported**.

By regularly running through, measuring, and monitoring the process, a **continuous improvement** process emerges. This ensures cybersecurity behavior is **sustainably integrated into daily practice**.

Impacts on Cybersecurity Behavior

Eleven Specific Influencing Factors

At NEXUS-7, we call the individual factors that influence behavior within the drivers "**impacts**." Impacts stimulate safe or unsafe behavior and operate on two levels:

1. Conscious Choices

- **Attitude:** Stance toward cybersecurity
- **Self-efficacy:** Confidence in one's own security behavior
- **Risk perception:** Assessment of threats

2. Automatic Responses

- **Habits:** Automated behavior
- **Stress reactions:** Behavior under pressure
- **Social influence:** Impact of colleagues and culture

The 11 Impact Areas

Each employee receives a score on these 11 impact areas, which provide specific points of engagement for targeted interventions:

1	**E-mail Security:**	Handling suspicious messages
2	**Password Management:**	Use and protection of credentials
3	**Social Engineering:**	Resilience against manipulation
4	**Data Protection:**	Handling confidential information
5	**Device Security:**	Securing devices
6	**Netwerk Security:**	Safe use of networks
7	**Software Updates:**	Timely updating of systems
8	**Physical Security:**	Physical security measures
9	**Incident Reporting:**	Reporting suspicious matters
10	**Compliance Adherence:**	Following rules and procedures
11	**Security Awareness:**	General security consciousness

Anchoring: From Insight to Habit

Impacts provide **concrete points of engagement** for interventions that help employees structurally anchor safe behavior.

Anchoring – making a new behavior or pattern **sustainable** – is essential for cybersecurity behavior, so that it becomes part of someone's **daily routines** and is automatically applied. A combination of both self-reflection and external support (coaching or training) ensures sustainable change.

NEXUS 7
RISK ASSESSMENT

The NEXUS-7 Advantages

Why Organizations Choose NEXUS-7

The NEXUS-7 approach offers demonstrable advantages over existing solutions:

✅ Deeper Insight into Human Behavior

In just 18 minutes, a complete personality profile across 7 levels and 11 impacts – much richer than traditional questionnaires.

✅ Predictive Power

Identify red flags before they lead to incidents. Proactive intervention instead of reactive response.

✅ Personalization at Scale

Unique insights per employee, combined with efficient clustering for organization-wide interventions.

✅ Faster Problem Detection

Real-time dashboards immediately show high-risk groups and trends, allowing you to act quickly.

✅ Improved Intervention Effectiveness

Targeted training based on data-driven insights increases effectiveness by 3-5x compared to generic awareness programs.

✅ Objective and Data-Driven

Scientifically grounded measurements eliminate subjectivity and bias from assessments.

✅ Continuous Optimization

Repeated measurements show measurable progress and adjust where necessary – a genuine improvement cycle.

Return on Investment

Direct Cost Savings:

- Prevention of one average data breach: €3.9 million
- Reduction in helpdesk calls through safer behavior: 15-30%
- Decreased downtime from malware infections: 40-60%
- Lower compliance fines through adherence: up to 4% of revenue

Indirect Value Creation:

- Strengthened customer trust and reputation
- Competitive advantage in security-sensitive sectors
- Improved employee engagement and safety culture
- Demonstrable compliance for audits and certifications

Rapid Implementation:
Operational within 2-4 weeks, first results visible within 1 month, positive ROI within 3-6 months

Implementation & Use

Four Steps to Successful Behavioral Change

Step 1: Baseline Measurement (Week 1-2)

- Roll out assessment to all employees
- Individual profiles and organizational overview
- Identification of red flags and risk groups

Step 2: Analysis & Planning (Week 3-4)

- Management workshops to discuss results
- Prioritization of interventions based on risk
- Development of personalized action programs

Step 3: Intervention & Training (Month 2-6)

- Execution of targeted training per cluster
- Individual coaching for high-risk employees
- Implementation of process and technical improvements

NEXUS7
RISK ASSESSMENT

Step 4: Monitoring & Optimization (Ongoing)

- Quarterly repeat measurements for progress
- Adjustment of interventions based on data
- Continuous improvement of security culture

Flexible Pricing for Every Organization

NEXUS-7 offers scalable, transparent pricing models that grow with your needs:

One-Time Assessments

Perfect for pilot projects or one-off measurements:

- Volume discount: the more tests, the lower the price per test
- From €25/test (small volumes) to €7.50/test (large volumes)
- 10 pricing tiers for optimal flexibility

Subscription Models

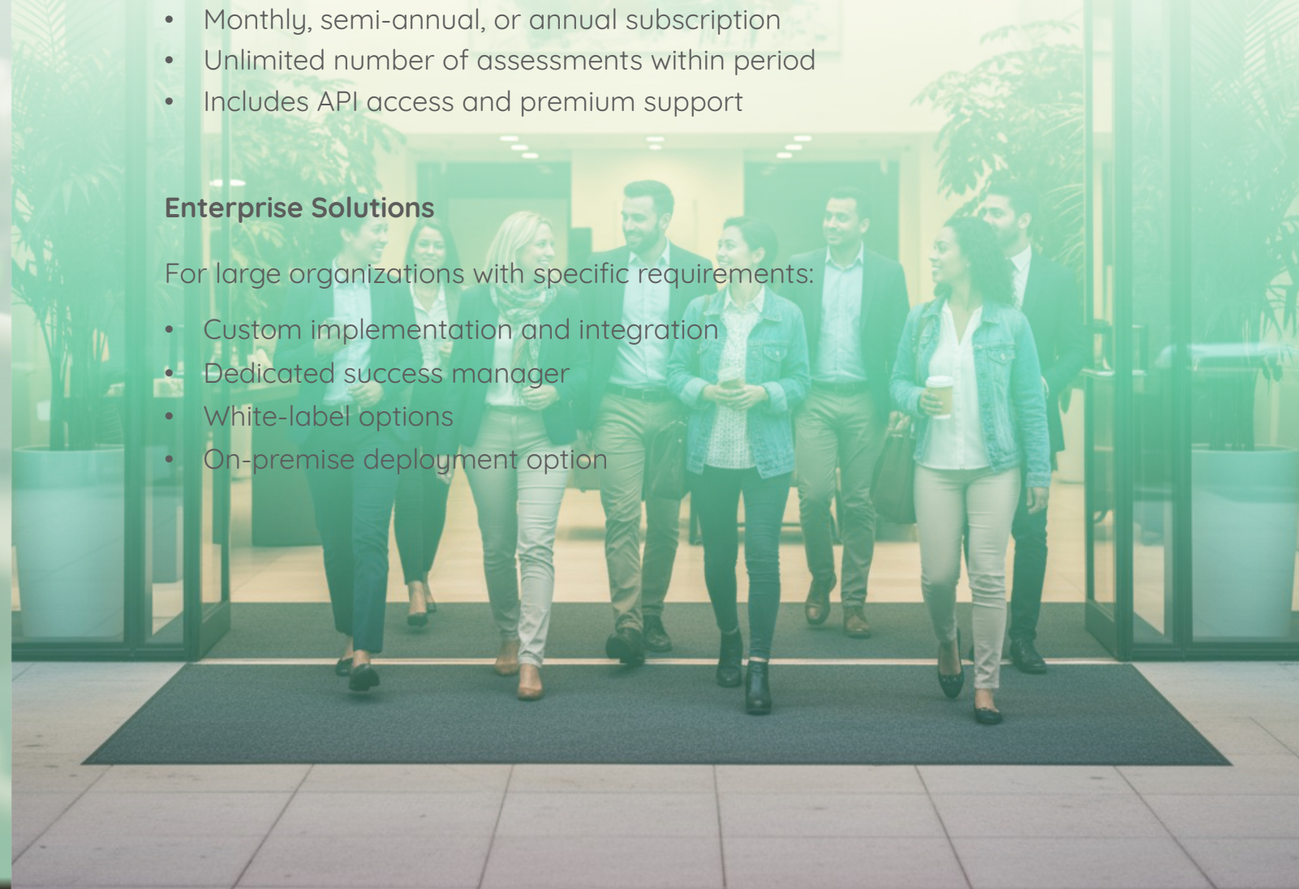
For organizations that want continuous monitoring:

- Monthly, semi-annual, or annual subscription
- Unlimited number of assessments within period
- Includes API access and premium support

Enterprise Solutions

For large organizations with specific requirements:

- Custom implementation and integration
- Dedicated success manager
- White-label options
- On-premise deployment option



NEXUS7
RISK ASSESSMENT

Who Is NEXUS-7 For?

Ideal Target Groups

NEXUS-7 is developed for organizations that take cybersecurity seriously and want to strengthen the human factor:

Large Enterprises (1000+ employees)

- Complex security landscape with diverse departments
- Need for continuous compliance and audits
- Budget for structural security investments

Medium-sized Organizations (100-1000 employees)

- Growing security needs without dedicated CISO
- Need for efficient approach with measurable results
- Focus on cost-effectiveness and ROI

Security-sensitive Sectors

- **Financial services:** banks, insurers, fintech
- **Healthcare:** hospitals, health insurers, medtech
- **Government:** ministries, municipalities, implementing organizations
- **Technology:** software companies, managed service providers
- **Industry:** manufacturing with critical infrastructure

Partners & Resellers

- **Security consultants** seeking added value
- **IT service providers** with security proposition
- **Training & development** organizations
- **HR advisors** focused on organizational development

NEXUS7
RISK ASSESSMENT

Technology & Platform

Modern SaaS Platform

NEXUS-7 is built by Roger Heykoop, Founder of Nexus-7, founder of various internet providers and former lead developer and lead architect of DigiD, as a state-of-the-art **Software-as-a-Service platform** with enterprise-grade security and scalability:

Technical Specifications

- **Multi-tenant architecture** for scalability
- **99.9% uptime SLA** with redundant infrastructure
- **GDPR-compliant** data processing and storage

Integration Capabilities

- **RESTful API** for custom integrations
- **SSO support** (SAML, OAuth) for seamless login
- **Export functionality** (PDF, Excel, CSV) for reports
- **Webhook notifications** for real-time updates
- **Embedding options** for white-label implementations

User Experience

- **Responsive design** for desktop, tablet, and mobile
- **Intuitive drag-and-drop interface** for Q-sort
- **Multi language support** (Dutch/English among others)
- **Accessibility compliant** (WCAG 2.1 AA)
- **Dark mode** for comfortable use

Security & Privacy

- **ISO 27001** certified infrastructure
- **End-to-end encryption** for sensitive data
- **Role-based access control (RBAC)** for data governance
- **Audit logging** for compliance tracking
- **Data residency** within EU

NEXUS7
RISK ASSESSMENT

Privacy and GDPR Compliance: Security without Compromise

Privacy by Design – not as an afterthought, but as a foundation.

At Nexus-7, security begins at the design stage: our system operates without personal data. Full stop. You determine how much privacy you wish to safeguard, from completely anonymous to identifiable – always with complete control.

Three Flexible Privacy Levels

Fully Anonymous Assessments

One invitation code, shared with your team. Employees receive a personal report, but no one else – including you – sees individual scores. Reports are exclusively at group level. Maximum privacy, actionable insights.

Traceable Assessments (with your own key)

Unique codes per employee, but the link remains in your hands. We see only codes; you manage the identity. Complete control without data leaving your systems.

Non-Anonymous Assessments (on request)

Do you prefer direct communication via email? We then use personal data exclusively for test administration and delete it automatically after reporting. A data processing agreement (GDPR-compliant) ensures everything is watertight.

Iron-Clad Guarantees

✅ **No selling, no sharing** – your data remains your data

✅ **EU-only hosting** – data never leaves the European Union

✅ **AI-proof** – no AI service gains access to client or employee data

✅ **On-premise available** – want Nexus-7 in your own data centre? We can arrange that.

Privacy isn't a feature. It's a mentality. And at Nexus-7, that mentality is central – so you can focus on what truly matters: the development of your team.

NEXUS7
RISK ASSESSMENT

Conclusion: Make Cybersecurity a Strength

From Weakest Link to Strongest Defense

Cybersecurity is much more than just technology – it depends largely on **human behavior**. Organizations can deploy any number of firewalls, antivirus programs, or advanced systems, but **true security is determined by** how **employees** handle information and digital processes on a daily basis.

NEXUS-7 offers an evidence-based, practical, and sustainable approach:

- **Actively supports employees** in making safe choices
- **Detects deviant behavior** (red flags) before it escalates
- **Helps identify and mitigate risks** in a timely manner
- **Transforms security** from compliance to culture

Start Today

Ready to Strengthen the Human Factor?

Transform your cybersecurity from a vulnerability into a strength. Contact us for a **no-obligation demo** or **pilot implementation** at your organization.

Contact:

Website: www.nexus-.nl

E-mail: info@nexus7.nl

The Three Pillars of Success

By combining **technology**, **behavioral science**, and **continuous improvement**, NEXUS-7 enables organizations to:

1. **Not just respond, but prevent** – proactive risk detection
2. **Not just train, but transform** – sustainable behavioral change
3. **Not just measure, but improve** – data-driven optimization

Make Cybersecurity an Integral Part

NEXUS-7 makes **cybersecurity** an **integral part of organizational culture and strategy**. Employees ultimately work on cybersecurity when they act **consciously**, **proactively**, and **consistently** according to best security practices, so that risks remain as small as possible and the organization is protected.

The NEXUS-7 Behavioral Analysis makes this a reality for your organization.Retry

Nexus-7
Lagedijk 11A
2064 KV Spaarndam
Nederland

+31 84 8332125
https://www.nexus-7.nl
info@nexus-7.nl