CyBehave

GOOD PRACTICE GUIDE

Human Risk Management

Turning Human Risk into Organisational Strength.

Publication Date: May 13th, 2025

Copyright Notice

Executive Summary

Human behaviour is now the most targeted and exploited element in cybersecurity breaches, yet also the most powerful defence when supported by the right strategy. This Human Risk Management Good Practice Guide provides a practical, strategic, and behaviourally grounded framework for identifying, managing, and mitigating human cyber risk within organisations.

Built around five core pillars - Governance & Leadership; Behavioural Insights & Measurement; Learning & Engagement; Cultural Reinforcement & Communication; and Incident and Learning Culture - the Good Practice Guide aligns globally recognised security frameworks (ISO/IEC 27001, NIST CSF) with the latest in behavioural science (COM-B, Behaviour Change Wheel, psychological safety).

The Good Practice Guide enables organisations to:

- ✓ Establish executive ownership and accountability for human cyber risk.
- ✓ Understand and address the fundamental behavioural drivers of insecure actions.
- ✓ Embed secure habits through contextual learning and cultural reinforcement.
- ✓ Foster a culture of psychological safety to promote open disclosure, learning, and continuous improvement.
- ✓ Measure progress using both leading and lagging behavioural indicators.

Each pillar includes maturity-based objectives and actions, allowing security leaders to assess current capability, prioritise development, and scale interventions over time. Supporting tools, including a roadmap and baseline checklist, along with policy template and behavioural indicators catalogue from our toolbox[1], provide a complete implementation toolkit.

This Good Practice Guide is designed for CISOs, security programme leads, human risk practitioners, and cross-functional stakeholders in HR, Risk, Communications, and Operations. It moves beyond awareness campaigns and technical controls, offering a holistic approach to embedding secure behaviour into the DNA of an organisation.

[1] Available at: https://professional.cybehave.org/toolbox/

Contents

Introduction

In today's digital environment, cyber threats increasingly exploit human vulnerabilities rather than technical weaknesses. Phishing, social engineering, poor password practices, misconfigurations, and procedural lapses are among the most common root causes of data breaches and operational disruptions. Traditional cybersecurity approaches that focus solely on technical controls or compliance-based awareness training are no longer sufficient.

The Human Risk Management Good Practice Guide offers a strategic, measurable, and culturally grounded framework for addressing the human dimension of cybersecurity. It integrates with globally recognised good practices, such as ISO/IEC 27001, the NIST Cybersecurity Framework, and ISO/IEC 27035, along with contemporary behavioural science models, including the COM-B model, the Behaviour Change Wheel, and principles of psychological safety.

This Good Practice Guide enables organisations to:

- ✓ Identify and understand behavioural drivers of cyber risk.
- ✓ Promote secure behaviour through capability-building, motivation, and social reinforcement.
- ✓ Establish trust and psychological safety to foster open disclosure and promote improvement.
- ✓ Embed secure practices into the daily rhythms, decisions, and culture of the organisation.
- ✓ Monitor and measure progress using behaviourally aligned metrics.

Framework

The structure of the Good Practice Guide is built around five core pillars that together form a comprehensive approach to reducing human cyber risk.

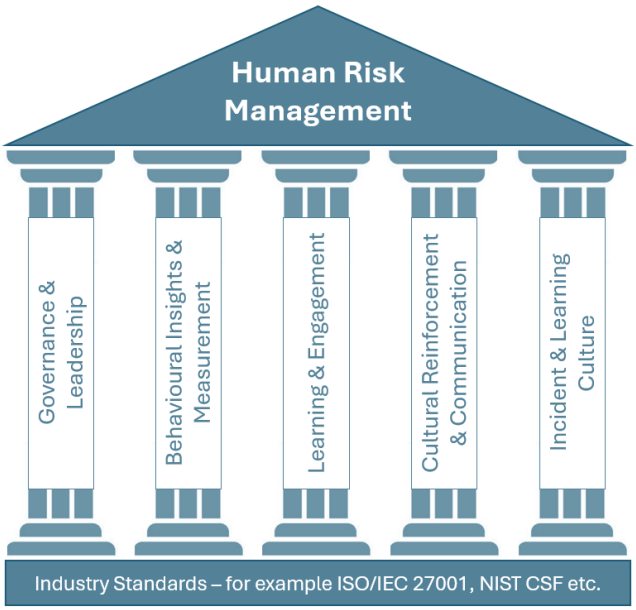

Figure 1: Human Risk Management Framework

These are:

1. Governance & Leadership
2. Behavioural Insights & Measurement
3. Learning & Engagement
4. Cultural Reinforcement & Communication
5. Incident & Learning Culture

Each pillar outlines clear objectives, implementation guidelines, and alignment with recognised security frameworks. Supporting sections provide tools and frameworks to help practitioners apply the Good Practice Guide, including a maturity model, an implementation roadmap, and a baseline checklist.

This Good Practice Guide is intended for use by CISOs, security programme leads, behavioural and cultural change professionals, and cross-functional stakeholders including HR, Communications, Risk, and Compliance. It promotes a collaborative, strategic approach to making secure behaviour the norm, not the exception.

Pillar 1: Governance & Leadership

Purpose: To ensure strategic ownership, visibility, and leadership commitment to human-centric cybersecurity.

Background & Role in the Bigger Picture: Governance and leadership define the tone and direction of organisational culture. Without senior-level buy-in and clear ownership, human risk often becomes a side issue. This pillar ensures human cyber risk is treated as a strategic business risk. It drives alignment across the organisation by embedding responsibilities and expectations at the top, where priorities and resources are shaped.

Common Challenges and How to Address Them

- **Lack of clarity around ownership**: Define human risk explicitly in risk registers and assign a named Executive Sponsor.
- **Leadership focuses on compliance over behaviour**: Educate leaders on the strategic value of behaviour change and how it links to resilience.
- **Low visibility of behavioural metrics**: Introduce human-centric dashboards into governance meetings and audit reports.

Objectives (Mapped to Maturity)

Maturity Level	Objectives
Developing	Human risk is acknowledged but not actively managed.
Defined	Executive Sponsor appointed. Governance boards regularly review human risk.
Managed	Human risk KPIs integrated into dashboards. Leaders model and reinforce secure behaviour.
Optimising	Human risk governance dynamically adapts in response to feedback and data.

Key Actions

- Appoint an Executive Sponsor.
- Create a human risk management policy
- Add human risk to strategic risk registers.
- Report human-related metrics at governance forums.
- Coach leaders on psychological safety and role-modelling.

Implementation Guidance

Why: Leadership sets priorities. If leaders do not visibly support human-centric security, the organisation will likely deprioritise it as well. Making this support explicit and ongoing ensures technical or regulatory concerns don't sideline human risk.

How:

- Executive Sponsor: Identify a C-suite advocate (e.g. COO, CIO) who has cross-functional influence. Their role is to champion investment in cultural and behavioural approaches, ensure accountability, and provide political cover for human-centred initiatives.
- Create a policy: Set clear direction on what is acceptable[2].
- Risk Registers: Collaborate with risk owners to clearly define human risk, using terms that align with enterprise risk management.
- Metrics Reporting: Develop and deliver a human risk dashboard for governance forums. Include both indicators (like incident trends) and cultural signals (like psychological safety scores).
- Leadership Coaching: Conduct brief sessions with leaders to increase awareness of psychological safety, behavioural modelling, and communication tone.

Industry Alignment

- ISO 27001: Clause 5.1, 5.3
- NIST CSF: ID.GV-1 to ID.GV-4

[2] Human Risk Management Policy template is available at: https://professional.cybehave.org/toolbox/

Pillar 2: Behavioural Insights & Measurement

Purpose

To use behavioural science to identify, analyse, and measure behavioural drivers of cybersecurity risk.

Background & Role in the Bigger Picture

Understanding behaviour is the foundation of effective intervention. This pillar allows organisations to move beyond compliance metrics and surface-level awareness tracking. It provides insight into what people are doing and why, so interventions can be more effective and better targeted.

Common Challenges and How to Address Them

- **Limited behavioural data:** Develop a data strategy that includes behavioural metrics like intent, confidence, and motivation.
- **Over-reliance on phishing or training stats:** Introduce complementary metrics such as near-miss reporting, response quality, and norm perceptions.
- **Disconnect between insight and action:** Link behavioural findings directly to intervention design using the COM-B model[3] [4].

Objectives (Mapped to Maturity)

Maturity Level	Objectives
Developing	Begin using phishing simulations and surveys.
Defined	Conduct COM-B behavioural diagnostics. Track leading/lagging indicators.
Managed	Integrate behavioural insights into dashboards. Use them to inform strategy.
Optimising	Dynamic behavioural analytics used to adapt security strategy in real time.

[3] Introduction to COM-B is available here: https://professional.cybehave.org/2025/05/13/practical-guide-to-com-b/

[4] Behavioural Change Playbook for Cybersecurity provides a detailed step-by-step application of COM-B and the Behaviour Change Wheel - https://amzn.eu/d/1CEZkrU

Key Actions

- Apply COM-B and BCW to identify behavioural drivers.
- Design interventions based on behavioural diagnostics.
- Create dashboards with indicators of capability, motivation, and opportunity.
- Link insights to action plans and governance.

Implementation Guidance

Why: Traditional metrics often measure surface-level actions (e.g. training completion) rather than behavioural intention or root cause. Behavioural measurement provides a deeper, more predictive insight into risk.

How:

- COM-B Diagnostic: Use simple surveys or facilitated interviews to determine whether staff have the Capability, Opportunity, and Motivation to exhibit secure behaviours. These can be targeted at specific roles or high-risk workflows.
- Behaviour Change Wheel (BCW): Use this framework to identify which functions (e.g. education, persuasion, enablement) are needed to change behaviour, based on diagnostic insights.
- Dashboards: Develop scorecards that blend quantitative (e.g. reporting rates, simulation performance) and qualitative (e.g. confidence levels, culture pulse) indicators. Regularly update and share them with governance forums.
- Link to Governance: Connect your insights to governance conversations. For example, show how a lack of motivation in frontline roles might increase susceptibility to phishing and recommend a targeted engagement plan.

Industry Alignment

- ISO 27001: Clause 9.1, ISO 27004
- NIST CSF: DE.CM-1, PR.AT-5

Pillar 3: Learning & Engagement

Purpose

To build secure behaviour through relevant, engaging, psychologically safe learning experiences.

Background & Role in the Bigger Picture

Security behaviours are shaped by how people are trained and supported. Effective learning isn't about information transfer; it's about creating the conditions for behaviour change. This pillar focuses on designing learning experiences that foster long-term habits and empower employees to act with confidence.

Common Challenges and How to Address Them

- **Generic, irrelevant content**: Tailor learning journeys to specific roles and behavioural risk profiles.
- **Low engagement**: Use interactive formats, storytelling, and scenarios to bring content to life.
- **Fear of failure inhibits learning**: Foster psychological safety by framing training as growth, not compliance.

Objectives (Mapped to Maturity)

Maturity Level	Objectives
Developing	Awareness campaigns and compliance eLearning.
Defined	Role-based, scenario learning has been introduced. Champions appointed.
Managed	Psychological safety is built into learning. Peer learning is active.
Optimising	Secure behaviours reinforced via nudges and embedded learning.

Key Actions

- Tailor learning by risk role and behavioural insight.
- Use simulations, storytelling, and nudges.
- Create safe spaces for discussion and reflection.
- Empower Champions to facilitate peer learning.

Implementation Guidance

Why: Generic or punitive training fails to address behavioural causes. Engaging, contextualised learning reinforces secure behaviour and increases retention and motivation.

How:

- Role-Tailored Learning: Utilise job role and behaviour diagnostics to identify the knowledge or habits that are missing. Focus learning on those gaps rather than a one-size-fits-all module.
- Storytelling & Simulations: Bring risks to life with scenario-based learning, phishing simulations, or user-generated stories that show both mistakes and successes.
- Psychological Safety: Avoid punitive messages. Create opportunities for reflection and discussion (e.g. workshops or informal Champion-led sessions) where people can safely admit confusion or mistakes.
- Nudges & Reminders: Use behavioural cues (e.g. just-in-time prompts, browser reminders, rewards) to help people remember secure behaviours at the point of action.

Industry Alignment

- ISO 27001: Clause 7.2–7.4
- NIST CSF: PR.AT-1 to PR.AT-5

Pillar 4: Cultural Reinforcement & Communication

Purpose

To sustain secure behaviour by embedding it in culture, communication, norms, and recognition.

Background & Role in the Bigger Picture

Behaviour change doesn't last unless it is culturally reinforced. This pillar ensures that secure behaviours become part of the organisation's identity - *"how we do things here."* It leverages internal communications, rituals, symbols, and leader narratives to promote alignment and a sense of belonging.

Common Challenges and How to Address Them

- **Disengaging messages:** Reframe communications using emotional language, social proof, and clear, concise language.
- **Lack of cultural visibility:** Use visual cues, values alignment, and stories to reinforce secure behaviour.
- **Behaviour not recognised:** Introduce informal recognition, such as team shout-outs and formal awards.

Objectives (Mapped to Maturity)

Maturity Level	Objectives
Developing	Reactive, technical communication.
Defined	Messaging framed using behavioural techniques. Campaigns aligned with culture.
Managed	Stories, rewards, and visual cues reinforce behaviour.
Optimising	Secure behaviour is embedded in language, rituals, and values.

Key Actions

- Use social proof and norm-based framing in all security messaging.
- Create rituals (e.g. monthly shout-outs, recognition boards).
- Align tone of voice and storytelling with organisational values.
- Make secure behaviour visible across channels and environments.

Implementation Guidance

Why: Culture and communication are what make secure behaviours stick. By aligning security with values, norms, and recognition, behaviours are more likely to become habitual and resilient.

How:

- Social Norms: Frame messages to reflect what the majority of people do or aspire to do. For example, “87% of employees reported phishing attempts last quarter.”
- Rituals & Recognition: Create small but consistent routines (like monthly "security shout-outs") that reinforce value in secure behaviour. Encourage peer nominations.
- Messaging Channels: Utilise existing communication channels — such as town halls, newsletters, and the intranet — to regularly share behavioural stories.
- Tone & Language: Avoid technical jargon. Use human stories, humour, and empathy to connect with audiences and promote a positive, security-aware identity.

Industry Alignment

- ISO 27001: Clause 7.4, Annex A.6
- NIST CSF: PR.IP-11, PR.AT-1

Pillar 5: Incident & Learning Culture

Purpose

To build trust and resilience by treating incidents as learning opportunities rather than sources of blame.

Background & Role in the Bigger Picture

How an organisation responds to incidents says everything about its culture. If people fear punishment, they won't report errors, which creates blind spots. This pillar supports early reporting, adaptive improvement, and system-level resilience through continuous learning.

Common Challenges and How to Address Them

- **Low reporting due to fear**: Introduce a psychological safety policy[5] that protects disclosers.
- **Blame-based culture**: Shift from "*who caused it*" to "*what enabled it*" in incident reviews.
- **Siloed lessons**: Share outcomes and improvements with all staff, not just response teams.

Objectives (Mapped to Maturity)

Maturity Level	Objectives
Developing	Reporting discouraged or ignored.
Defined	Reporting tools and guidance are in place. No-blame policy introduced.
Managed	Behavioural root cause reviews conducted. Lessons shared.
Optimising	High-trust environment. Mistakes trigger system-level improvements.

[5] Template available here: https://professional.cybehave.org/toolbox/

Key Actions

- Introduce a psychological safety policy and effective communication strategies.
- Train responders and leaders on how to handle disclosure.
- Apply COM-B to incident review.
- Share learnings organisation-wide through stories, not just metrics.

Implementation Guidance

Why: When staff fear punishment, they stay silent, which prevents learning and perpetuates risk. Treating incidents as learning opportunities increases early reporting and systemic improvement.

How:

- Psychological Safety Policy: Communicate a clear, leadership-endorsed stance that reporting mistakes in good faith will not lead to disciplinary action.
- Responder Training: Equip SOC analysts, managers, and HR with scripts and mindset tools to respond to incident disclosures constructively and without blame.
- Root Cause Analysis (RCA): Add behavioural analysis (using COM-B) to RCA templates. For example, if someone shared credentials, assess whether they lacked the capability (e.g., a misunderstanding of policy), opportunity (e.g., system constraints), or motivation (e.g., fear of delay).
- Story-Based Sharing: Use anonymised case studies or retrospectives in newsletters, team briefings, or learning platforms to spread awareness and reduce stigma.

Good Practice Guides Alignment

- ISO 27001: Clause 10.1, ISO 27035
- NIST CSF: RS.AN-1, RS.IM-1

Baseline Checklist

The baseline checklist is designed to help organisations assess their current human risk management practices against the five pillars of the guidance. It provides a quick diagnostic to identify areas of strength and those needing development.

Instructions: Review each item and mark your organisation's current status using the scoring guide below.

Scoring Guide

- **Yes (2 points)** – Fully in place and consistently applied
- **Partial (1 point)** – In progress or inconsistently applied
- **No (0 points)** – Not yet started or not applicable

Section / Item	Score	Notes
Pillar 1: Governance & Leadership		
Executive Sponsor for human risk appointed		
Human risk is discussed in governance forums		
KPIs on human risk are included in dashboards		
Leaders trained on secure behaviour and psychological safety		
Human risk is integrated into strategic risk planning		
Pillar 2: Behavioural Insights & Measurement		
Behavioural diagnostics (e.g. COM-B) conducted		
Behavioural risk indicators are tracked and reported		
Behavioural data used to inform security strategy		
Leading and lagging metrics implemented		
Behavioural insights shared with key stakeholders		
Pillar 3: Learning & Engagement		
Role-specific, scenario-based training delivered		
Psychological safety embedded in learning environments		
Champions or peer advocates are actively engaged		
Behavioural objectives included in the learning design		
Learning outcomes are evaluated beyond completion rates		
Pillar 4: Cultural Reinforcement & Communication		
Security messaging framed with behavioural science		

Secure behaviours are publicly recognised and rewarded		
Leadership visibly supports security culture		
Cultural feedback is collected regularly (e.g. surveys)		
Security norms reinforced via rituals or storytelling		
Pillar 5: Incident & Learning Culture		
Psychological safety policy supports reporting		
Behavioural root cause analysis conducted on incidents		
Near-miss and informal reporting encouraged		
Lessons learned are shared across the organisation.		
Incident trends used to inform training and policies		

Scoring Summary	Total Score (Max 10)	Priority Action Required?
Governance & Leadership		
Behavioural Insights & Measurement		
Learning & Engagement		
Cultural Reinforcement & Communication		
Incident & Learning Culture		

Interpretation Guide

The interpretation of scores is straightforward: a total of 8–10 indicates a strong foundation is in place; 5–7 reflects a progressing area with clear opportunities for improvement; and 0–4 highlights a priority area requiring focused development.

This checklist should be used as a diagnostic tool at regular intervals, such as quarterly or annually, to inform planning, track progress toward maturity, and demonstrate value to leadership.

Implementation Roadmap

The implementation roadmap provides a phased approach to embedding the Human Risk Management Good Practice Guide. It is structured around the **five defined maturity levels**: *Initial*, *Developing*, *Defined*, *Managed*, and *Optimising*. Each level includes pillar-specific activities that help organisations move toward maturity.

Level 1: Initial

Objective: Human risk is not yet formalised. The focus is on raising awareness and recognising the gap.

Pillar	Key Activities
Governance & Leadership	No formal ownership of human risk. Ad hoc leadership mentions without accountability. Identify the need for executive sponsorship.
Behavioural Insights & Measurement	No behavioural data or diagnostic tools. Begin to explore behaviour as a risk vector.
Learning & Engagement	Basic compliance-based training only. Assess current training relevance and limitations.
Cultural Reinforcement & Communication	Communications are reactive and technical. Identify opportunities for cultural alignment.
Incident & Learning Culture	Incidents are reviewed technically. No behavioural root cause analysis. Begin cultural conversations on mistakes.

Level 2: Developing (0–6 months)

Objective: Lay foundations for governance, diagnostics, and behaviourally aware learning.

Pillar	Key Activities
Governance & Leadership	Appoint Executive Sponsor; Begin reporting human risk to governance forums.
Behavioural Insights & Measurement	Conduct initial COM-B diagnostics; Define basic behavioural metrics and baselines.
Learning & Engagement	Audit existing training; Develop initial role-based training content; Identify Security Champions.
Cultural Reinforcement & Communication	Launch introductory human risk communications; Frame messages using social proof and plain language.
Incident & Learning Culture	Promote no-blame philosophy; Encourage informal reporting and begin sharing anonymised lessons.

Level 3: Defined (6–12 months)

Objective: Establish structured programmes, measurement, and cross-functional ownership.

Pillar	Key Activities
Governance & Leadership	Formalise human risk KPIs; Integrate into risk dashboards and leadership reviews.
Behavioural Insights & Measurement	Broaden diagnostics; track both leading and lagging indicators; link insights to effective interventions.
Learning & Engagement	Roll out contextualised training; Launch Champion-led learning activities.
Cultural Reinforcement & Communication	Align communications with values; use rituals (e.g., shout-outs) to reinforce norms.
Incident & Learning Culture	Begin structured behavioural root cause reviews; Create feedback loop into training and comms.

Level 4: Managed (12–24 months)

Objective: Embed human risk into governance, planning, and continuous improvement cycles.

Pillar	Key Activities
Governance & Leadership	Link human risk outcomes to leadership performance and adapt strategy based on the data.
Behavioural Insights & Measurement	Establish behavioural dashboards; Include insights in governance decision-making.
Learning & Engagement	Evaluate training based on behavioural change, not just completion; Align learning with incident trends.
Cultural Reinforcement & Communication	Scale behavioural branding; Highlight positive norms and behaviours across channels.
Incident & Learning Culture	Share organisation-wide incident lessons; Assess psychological safety in culture surveys.

Level 5: Optimising (24+ months)

Objective: Human risk management is a dynamic, predictive, and continuously refined process.

Pillar	Key Activities
Governance & Leadership	Embed human risk in strategic planning and investment decisions.
Behavioural Insights & Measurement	Automate behavioural insight collection; benchmark and adjust interventions in real-time.
Learning & Engagement	Fully embed learning into daily work (e.g. nudges, habit loops); Track long-term impact.
Cultural Reinforcement & Communication	Secure behaviour is part of identity and rituals; Culture-led peer influence reinforced.
Incident & Learning Culture	Psychological safety institutionalised; Behavioural learnings influence future controls and policy.

This roadmap provides a clear path from informal beginnings to embedded behavioural excellence. It should be reviewed annually and used to prioritise activities aligned to maturity aspirations.

Action Plan

The most significant vulnerabilities and the greatest opportunities for resilience lie in human decisions, behaviours, and culture. The **Human Risk Management Good Practice Guide** provides a practical, behavioural, and strategic foundation to address these challenges head-on.

By applying the five interconnected pillars, organisations can move beyond checkbox awareness to build a culture where secure behaviour is understood, supported, measured, and continuously improved. This is not about perfection — it's about progress, empowerment, and creating an environment where every employee contributes to a safer organisation.

The successful implementation of this guidance requires a leadership commitment, cross-functional collaboration, and a willingness to foster a psychologically safe environment and promote adaptive learning. As threats evolve, so too must our human defences — grounded in insight, guided by science, and driven by culture.

Next Steps:

- Assess your organisation against the baseline checklist.
- Prioritise action using the maturity model.
- Use the implementation roadmap to guide delivery.
- Align interventions to behavioural diagnostics and real-world risks.
- Continuously measure, reflect, and adapt.

By turning human risk into human strength, we build not just secure systems, but resilient, security-conscious organisations.

For further tools, insights, and resources on human risk management and cybersecurity culture, visit **www.cybehave.com**.

CyBehave offers a wide range of practitioner guides, learning journeys, behavioural toolkits, and leadership resources to support organisations at every stage of their human cyber risk maturity. Join our growing community of security and change leaders who are working to empower a more secure, cyberwise society.