cyberwhy



SERVICE GUIDE

Cyber Security Consulting

How to turn risk and requirements into a security plan you can carry out, from strategy to standards.

01 · OVERVIEW

Why it matters

Security consulting turns a vague worry into a plan. It starts with your business: what you must protect, what could go wrong and what customers, partners and regulators expect of you. From there it builds the strategy, the policies and the path toward standards.

Good consulting is not a thick document. It is a short list of decisions, an owner for each, and a rhythm that keeps security current as the business changes.

Typical triggers

- Customers send security questionnaires and answers are assembled by hand each time
- You are preparing for ISO 27001 or for GDPR requirements
- Security grew organically and no one owns the whole picture
- A new product, market or acquisition changes your risk
- You are starting to use AI and need rules for it
- Management asks: are we secure enough, and how would we know?

Who benefits

CEO or owner

A clear view of risk, in business terms.

CIO or IT manager

A roadmap that matches budget and capacity.

Compliance lead

A path toward ISO 27001 and GDPR requirements.

Security lead

Policies and standards that people actually follow.

In this guide

01 Overview 2
02 What it is, and what it is not 3
03 How it works, step by step 4
04 What you receive 5
05 In practice 6
06 How to prepare 8
07 Questions, references and terms 9
08 How the services fit together 10

02 · SCOPE

What it is, and what it is not

What it is

- + Tailored to your organization, whether improving what exists or building new
- + Risk-based: effort goes where the risk is
- + Practical: policies and plans people can follow
- + Continuous: guidance continues as your needs change

What it is not

- – Not certification: certification is awarded by accredited bodies
- – Not a generic template pack with your logo on it
- – Not a one-off document that is filed and forgotten
- – Not a replacement for testing or monitoring

What consulting covers

Security strategy

Goals, priorities and a roadmap that fit your business, with clear owners and a sensible order of work.

Risk assessment

A structured look at assets, threats and weaknesses, rated by likelihood and impact, so decisions rest on evidence.

Security policies

The rules behind the strategy: who may access what, how data is handled and what happens when something goes wrong.

Standards and compliance

Guidance toward standards such as ISO 27001 and GDPR requirements, including gap analysis and preparation.

Ongoing guidance

A regular rhythm of review, so security stays current as systems, people and threats change.

03 · PROCESS

How it works, step by step

A typical engagement, from the first conversation to clear next steps. Exact steps and timing are agreed with you when the work is scoped.

01 Discuss

Understand your business, risks and requirements.

- Talk through your products, customers, data and growth plans
- Collect the requirements you face: contracts, regulations, customer questionnaires
- Learn what exists already: policies, tools, responsibilities

YOU PROVIDE
Business context, risks and requirements
Existing documents and tools

YOU GET
A shared starting point

02 Assess

Show where you are today.

- Identify the assets that matter: data, systems, processes
- Describe threats and weaknesses, and rate risks by likelihood and impact
- Compare the current state with your goals and requirements

YOU PROVIDE
Access to people who know the systems and processes
Honest answers about gaps

YOU GET
A clear picture of where you are today

03 Plan

Decide what to do, in which order.

- Define a security strategy tailored to your organization
- Choose how to treat each risk: reduce, transfer, avoid or accept
- Write the security policies behind the strategy
- Build a roadmap with owners and priorities

YOU PROVIDE
Decisions on priorities and risk appetite
Reviews of draft policies

YOU GET
A strategy and the policies behind it

04 Align

Prepare for the standards you need.

- Map your controls to ISO 27001 and GDPR requirements
- Find gaps and plan how to close them
- Prepare evidence and documentation for the standard

YOU PROVIDE
Responsible people for each area
Evidence of controls already in place

YOU GET
Guidance toward the standard

05 Support

Keep security current.

- Review risks and progress at an agreed rhythm
- Advise on changes: new systems, suppliers, products
- Adjust policies and priorities as needs change

YOU PROVIDE
Early notice of changes that affect security

YOU GET
Ongoing guidance to keep security current

04 · DELIVERABLES

What you receive

The outcome is a set of working documents and decisions: what you protect, why, who is responsible and what happens next. Each can be shown to a customer, an auditor or a new colleague.

01
Risk assessment
Assets, threats and weaknesses, rated and ranked.

02
Security strategy
Goals, principles and a roadmap with priorities and owners.

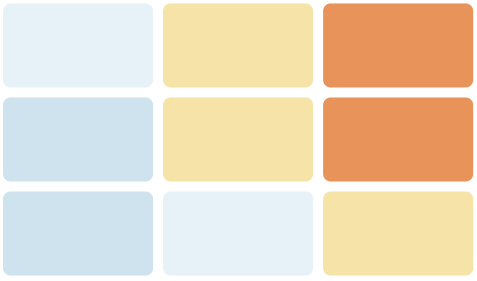
03
Policy set
The rules for access, data, suppliers, incidents and more, tailored to you.

04
Gap analysis
Where you stand against ISO 27001 and GDPR requirements.

05
Roadmap
What to do first, next and later, in realistic steps.

06
Ongoing guidance
Regular reviews and advice as things change.

A simple risk matrix



Likelihood → (columns) · Impact ↑ (rows)

Risks are rated by how likely they are and how bad the impact would be. The color shows how urgently to act. Each risk then gets a decision and an owner.

05 · IN PRACTICE

Seeing it at work

The road toward ISO 27001

1	**Scope and context**	Define what the management system covers and who cares about it.
2	**Risk assessment**	Identify and rate risks, and decide how to treat them.
3	**Select controls**	Choose controls from Annex A and record them in the Statement of Applicability.
4	**Implement**	Put controls, policies and responsibilities in place and train people.
5	**Check**	Run an internal audit and a management review.
6	**Certify**	An accredited certification body audits and decides. Guidance toward the standard is not certification.

Typical policy set

- Information security policy
- Access control and passwords
- Acceptable use of systems and AI tools
- Data classification and handling
- Incident response plan
- Backup and recovery
- Supplier and third-party security
- Secure development and change management

A rhythm that keeps security current

1. **Review** — Look at risks, incidents and changes on a regular schedule.
2. **Decide** — Update priorities and owners, and record accepted risks.
3. **Adjust** — Change policies and controls to match the decisions.
4. **Report** — Give management a short, honest picture of progress.

05 · IN PRACTICE

Good to know

GOOD TO KNOW

ISO 27001 and GDPR in brief

Standards

ISO/IEC 27001	A standard for an information security management system. The 2022 edition lists 93 controls in four themes: organizational, people, physical and technological.
GDPR	A law for personal data. Its principles include data minimization, integrity and confidentiality, and accountability. Article 32 requires appropriate security of processing.
THE DIFFERENCE	ISO 27001 is a voluntary management standard you can be certified against. GDPR is a legal requirement without a certificate.

FOR AI PROJECTS

Consulting for projects that use AI

AI changes the risk picture: data leaving through prompts, models and components from outside suppliers, and agents with broad permissions. Good guidance gives you a short AI policy, a risk register that includes these topics and clear rules on which data may go into which tool. Frameworks such as the NIST AI Risk Management Framework and ISO/IEC 42001 can serve as reference.

06 · PREPARATION

How to prepare

A little preparation makes the work faster, safer and more useful. Here is what helps most.

Before we start

- Name an executive sponsor
- Collect existing policies, contracts and customer questionnaires
- List the systems, suppliers and data types that matter most
- Know which standards or laws apply to you
- Make people available for interviews
- Decide how much change the organization can absorb

Typical ground rules

- + Recommendations fit your size, budget and capacity
- + Policies are written to be read and followed
- + You keep ownership of decisions and risk acceptance
- + Guidance toward a standard is not certification

Common misconceptions

~~Compliance equals security.~~	**In practice:** Standards set a floor and a process. Real security needs risk-based decisions beyond the checklist.
~~We are too small for ISO 27001.~~	**In practice:** The standard scales with the organization. The scope can start small and grow.
~~Policies are paperwork.~~	**In practice:** Policies that match how people work reduce mistakes and shorten audits and questionnaires.

07 · REFERENCE

Questions, references and terms

Frequently asked questions

Where do we start?
With a conversation about your business, risks and requirements. From that, a risk assessment shows where you stand.

Will you certify us for ISO 27001?
No. Certification is awarded by accredited bodies. We guide you toward the standard.

Do we need consulting if we are not pursuing a standard?
Yes, if you want a plan. Strategy, risk assessment and policies are valuable on their own.

Can you help with customer questionnaires?
A clear policy set and documented risks make answers faster and more consistent.

How does AI fit in?
AI is treated like any other change to your risk: assets, data flows, suppliers and owners, with a few specific rules.

How often do we review?
At a rhythm you agree, and whenever something significant changes.

Reference frameworks and sources

ISO/IEC 27001 and 27002	The management standard and its catalog of controls.
GDPR (EU 2016/679)	The EU regulation on personal data protection.
NIST Cybersecurity Framework 2.0	A framework with six functions: Govern, Identify, Protect, Detect, Respond and Recover.
CIS Critical Security Controls	A prioritized set of practical safeguards.
NIST AI RMF and ISO/IEC 42001	Frameworks for managing risks of AI.

Terms in plain language

Risk appetite. How much risk the organization is willing to accept.

Gap analysis. A comparison of the current state with a requirement.

Statement of Applicability. The list of controls chosen under ISO 27001, with reasons.

Control. A safeguard that reduces a risk: a rule, a process or a technology.

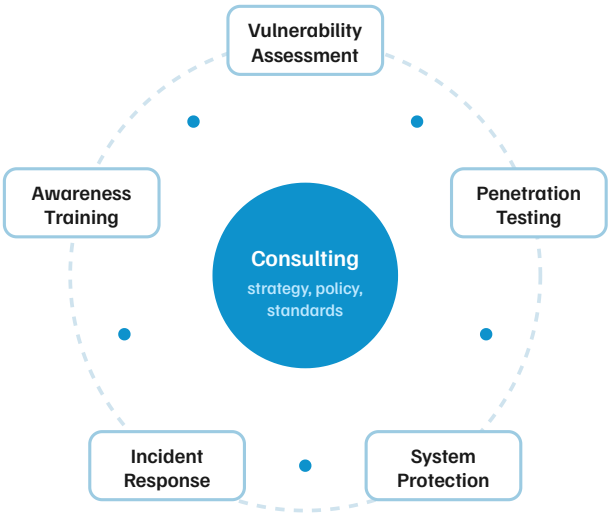
ISMS. Information security management system, the core of ISO 27001.

Accredited body. An independent organization authorized to certify against a standard.

08 · NEXT STEPS

How the services fit together

Security works best as a cycle: find weaknesses, test them, protect, prepare to respond and keep people alert, all guided by a strategy. You can start with any one of them.



Vulnerability Assessment
Finds known weaknesses across your systems and ranks them.

Penetration Testing
Shows what an attacker can actually exploit.

System Protection
Closes gaps with layered, maintained defenses.

Incident Response and Forensics
Acts when something gets through, and learns from it.

Security Awareness Training
Prepares the people who meet threats first.

Cyber Security Consulting (this guide)
Sets strategy, policy and standards that tie it together.

Talk to a specialist about cyber security consulting.

Tell us what you are working on and what you need to protect.

EMAIL
info@cyberwhy.com

WEB
cyberwhy.com/services/cyber-security-consulting/

This guide describes how work of this kind typically runs. Scope, methods, timing and deliverables are agreed with you for your situation, and nothing in it is a guarantee. References to standards and frameworks are for orientation and do not mean certification. © CyberWhy. All rights reserved.