# Information Security Management System ISO/IEC 27001

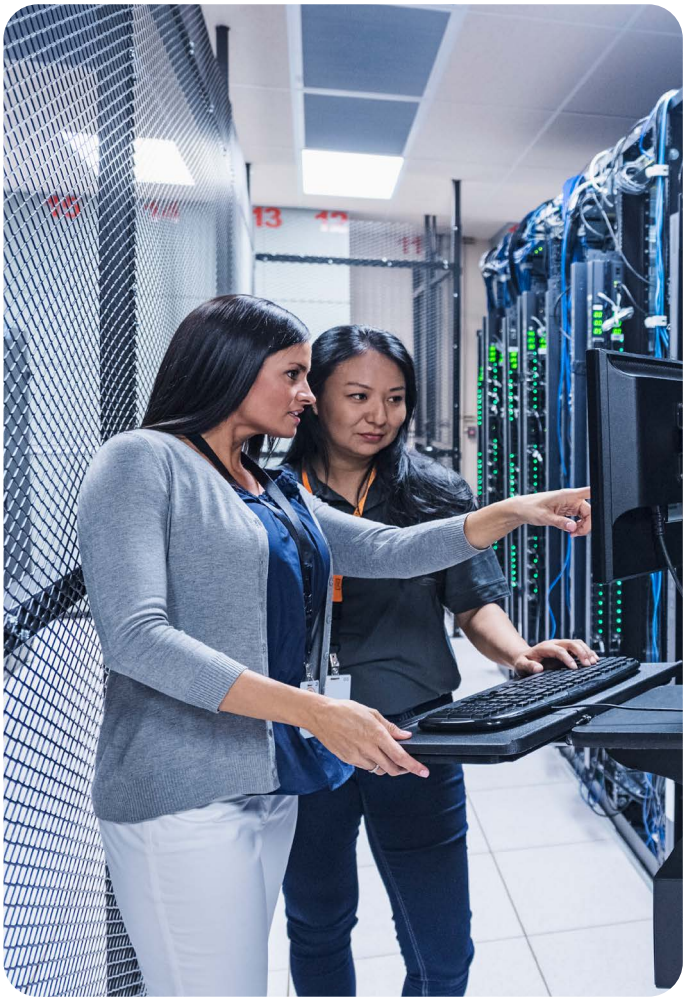
## Self-assessment checklist

Your partner in progress

## Where is your organization on the path to information security management maturity?

Increasing reliance on digital tools, technologies, and services throughout the supply chain is driving the need for greater information security and cybersecurity attention.

With a mature and certified Information Security Management System (ISMS) in place, organizations can keep the data they are responsible for safe, as well as unlock additional advantages for the future. This includes effectively protecting customers and minimizing risk, to opening doors to new growth opportunities, regardless of industry or region.



## Introducing ISO/IEC 27001 – Information Security Management System

Globally recognized best practice, ISO/IEC 27001, provides the robust framework and flexibility you need to manage and protect your information. It helps you continually review and refine your processes, building information security resilience today, while ensuring readiness for tomorrow.

## The benefits of certification

Independent certification demonstrates your organization's commitment to excellence. By gaining third-party assurance that your information security management system (ISMS) meets the requirements of ISO/IEC 27001, you can inspire confidence in your ability to safeguard your information assets, mitigate risks, and build trust with an internationally recognized mark of excellence.

## Clauses included in this self-assessment

Clause 4 - Context of the Organization

Clause 5 - Leadership

Clause 6 - Planning

Clause 7 - Support

Clause 8 - Operation

Clause 9 - Performance Evaluation

Clause 10 - Improvement

## How the self-assessment works

By filling in the checklist on the next few pages you can gauge what stage of maturity your ISMS is currently at in relation to the main requirements of the standard, and what actions you can take next. No matter where you are in your digital trust journey, our range of solutions can help you move forward.

*Please fill in the checklist below, each 'yes' counts as one point towards your final score and subsequent maturity range.*

## Snapshot of our ISMS maturity scores

### Early stage

**0-13 Points:**

Begin with our digital trust courses and qualifications to solidify your foundational knowledge and practical skills in managing information security.

Learn more

### Moderate stage

**14-21 Points:**

Consider a BSI Gap Assessment to align your current practices with future goals, enhancing performance through standards.

To achieve maturity, our courses and qualifications should be key considerations.

Learn more

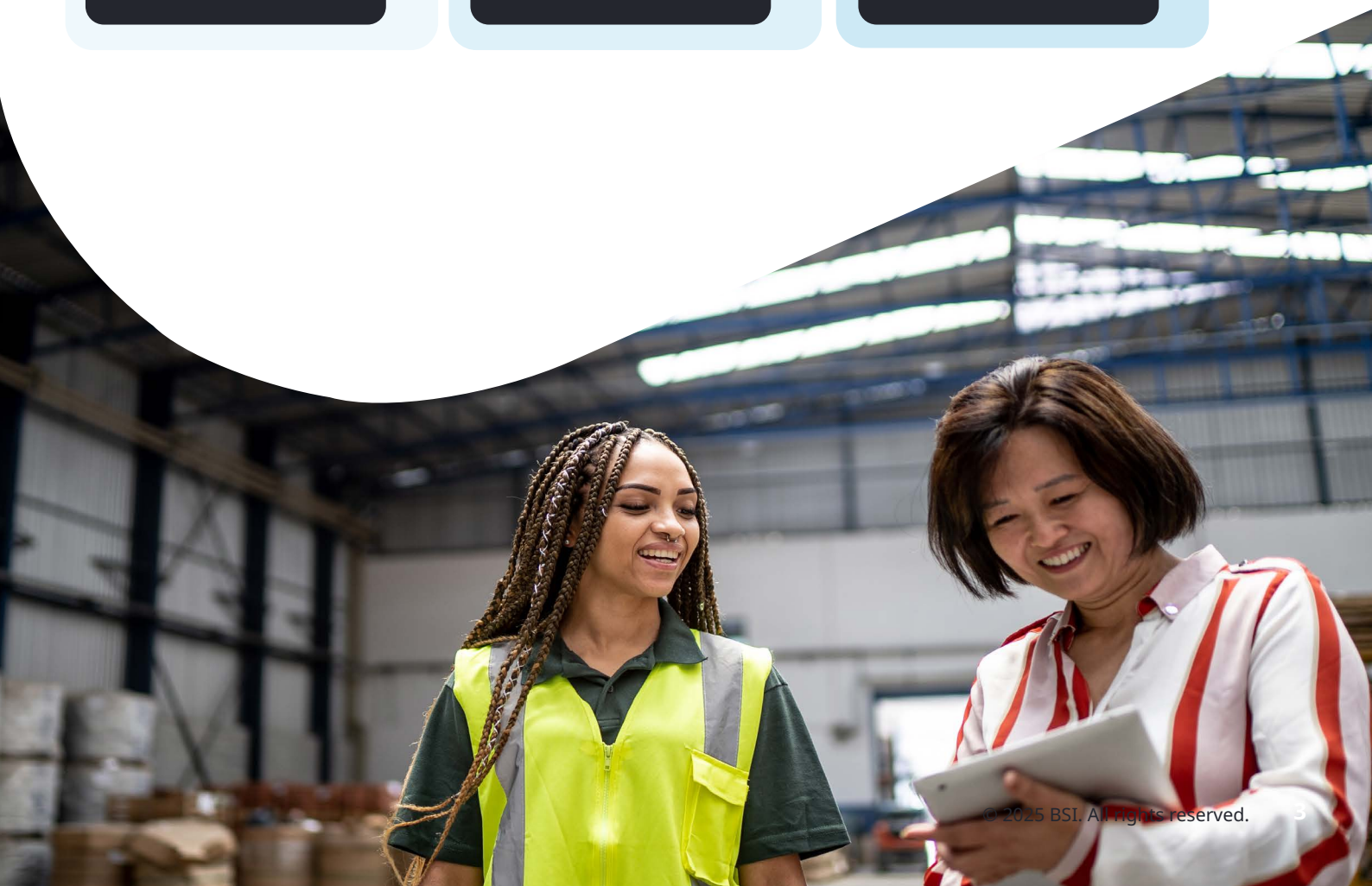
### Mature stage

**22-29 Points:**

Pursue ISO/IEC 27001 certification to distinguish your ISMS, confirming and demonstrating your industry leading digital trust and information security practices.

Training courses for the continued development of staff will also help you achieve full-scale maturity.

Learn more



# Your ISMS self-assessment checklist

## Clause 4 - Context of the Organization

| | | Yes | No |
|---|---|---|---|
| 1 | Have you looked at what's happening inside and outside your organization, and what customers, regulators, and other interested parties expect when it comes to information security? Including whether climate change is a relevant issue. | ☐ | ☐ |
| 2 | Have you decided which of those expectations and requirements your information security system should meet? | ☐ | ☐ |
| 3 | Have you clearly defined what parts of your organization are included in your information security system scope, including work done by others or partners and their requirements related to climate change? | ☐ | ☐ |
| 4 | Have you set up the main activities, responsibilities, and improvements needed to keep your information security system working well over time? | ☐ | ☐ |

## Clause 5 - Leadership

| | | | |
|---|---|---|---|
| 5 | Does your organization have an information security policy and goals that support your overall direction and have they been shared with your team and key stakeholders? | ☐ | ☐ |
| 6 | Have clear roles and responsibilities been assigned to manage and support the information security system, with the authority to act and report on its performance? | ☐ | ☐ |
| 7 | Has leadership made sure there's a plan in place to meet the information security goals, and that everyone understands why it matters and how to contribute? | ☐ | ☐ |

Continued ›

Reset checklist

# Your ISMS self-assessment checklist

## Clause 6 - Planning

| | | Yes | No |
|---|---|---|---|
| 8 | Have you identified the main risks and opportunities that could affect your information security system, and planned how to address them? | ☐ | ☐ |
| 9 | Do you have a clear and repeatable process to assess information security risks, including how likely they are and what impact they could have? | ☐ | ☐ |
| 10 | Have you set rules for accepting risks, and are risk levels prioritized based on those rules? | ☐ | ☐ |
| 11 | Have you identified who is responsible for each risk and made sure they review and approve any risk plans? | ☐ | ☐ |
| 12 | Have you chosen and applied the right actions or controls to reduce risks, and checked them against the controls listed in Annex A of ISO/IEC 27001 to see whether any relevant controls have been missed? | ☐ | ☐ |
| 13 | Do you have a Statement of Applicability that details all the controls that have been selected, which Annex A controls are used, why they were chosen or excluded, why any additional controls were included and whether they've been implemented? | ☐ | ☐ |
| 14 | Do you have a risk treatment plan in place, and are any remaining (residual) risks clearly accepted by the right people? | ☐ | ☐ |
| 15 | Have you set clear, measurable goals for your ISMS, and shared them with the right people across your organization? | ☐ | ☐ |
| 16 | When planning changes to your ISMS, do you have a process to make sure updates are managed in an organized way? | ☐ | ☐ |

Continued ›

# Your ISMS self-assessment checklist

## Clause 7 - Support

| | | Yes | No |
|---|---|---|---|
| 17 | Have you provided the people, tools, and environment needed to run and improve your information security system? | ☐ | ☐ |
| 18 | Are the people in ISMS-related roles properly trained and do they understand their responsibilities, the policy, and why their actions matter? | ☐ | ☐ |
| 19 | Is your information documented, protected, and shared in the right way—and are communications with internal and external parties clearly defined? | ☐ | ☐ |

## Clause 8 - Operation

| | | | |
|---|---|---|---|
| 20 | Have the planned actions to manage risks and opportunities been built into your daily processes and are those processes followed as intended? | ☐ | ☐ |
| 21 | When changes are needed, do you manage them in a careful and planned way to avoid unwanted impacts on information security? | ☐ | ☐ |
| 22 | Are any outsourced or third-party services properly managed to meet your information security requirements? | ☐ | ☐ |
| 23 | Do you regularly assess information security risks and keep records of those assessments, treatment decisions, and approvals? | ☐ | ☐ |

Continued ›

Reset checklist

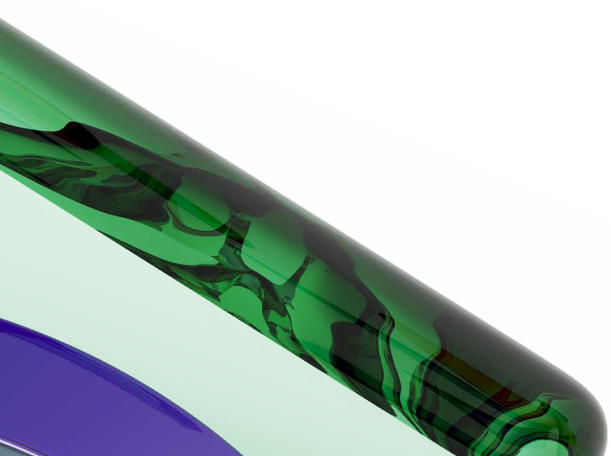
# Your ISMS self-assessment checklist

## Clause 9 - Performance Evaluation

| | | Yes | No |
|---|---|---|---|
| 24 | Have you defined what needs to be measured, how, when, and by whom—and do you keep records of the results? | ☐ | ☐ |
| 25 | Do you carry out internal audits using impartial auditors, and are the results reported to management and documented? | ☐ | ☐ |
| 26 | Is there a process in place to address any problems or nonconformities found during monitoring or audits? | ☐ | ☐ |
| 27 | Do you carry out internal audits using impartial auditors, and are the results reported to management and documented? | ☐ | ☐ |
| 28 | Have you defined what needs to be measured, how, when, and by whom—and do you keep records of the results? | ☐ | ☐ |

## Clause 10 - Improvement

| | | | |
|---|---|---|---|
| 29 | When something goes wrong, do you take action to fix it, find and correct the root cause, check that the fix worked, and keep a record of what was done? | ☐ | ☐ |



## Your score

0

Reset checklist

- Scored 0-13 points
- Scored 14-21 points
- Scored 22-29 points

**If you scored 0-13 points...**

## Elevate your ISMS skills and knowledge with courses & qualifications from BSI

Based on your organization's maturity score, we'd recommend exploring our dedicated information security courses and qualifications for you and your team.

Developed in conjunction with leading industry experts, our information security training courses provide the most relevant and up-to-date skills and knowledge. Our courses can help you to interpret and understand the standard requirements and how to audit the management system. We also offer courses focused on key skills that bolster your abilities and knowledge as a security professional, such as cybersecurity, data and privacy, AI, cloud security, and more.

Wherever you are on your journey, whatever your role, we have a course to help you be more efficient at what you do.

Explore our courses and qualifications ›

**If you scored 14-21 points...**

## Elevate your ISMS with a BSI Gap Assessment

Based on your organization's maturity score, you may benefit from a Gap Assessment from our expert auditors ahead of pursuing certification.

A Gap Assessment with BSI provides you with a method of assessing your current situation against future goals, pinpointing areas where your existing program does not meet the requirements of ISO/IEC 27001. Our auditors are uniquely positioned to help you, thanks to their significant experience and expertise in information security management across many industry sectors. Following your assessment, you'll have information to act upon taking your ISMS maturity to the next level, progressing your organization towards achieving ISO/IEC 27001 certification.

Visit our website to find out more ›

Getting the right skills and knowledge embedded in your organization will enhance your ISMS. Explore our courses and qualifications **here**.

**If you scored 22-29 points...**

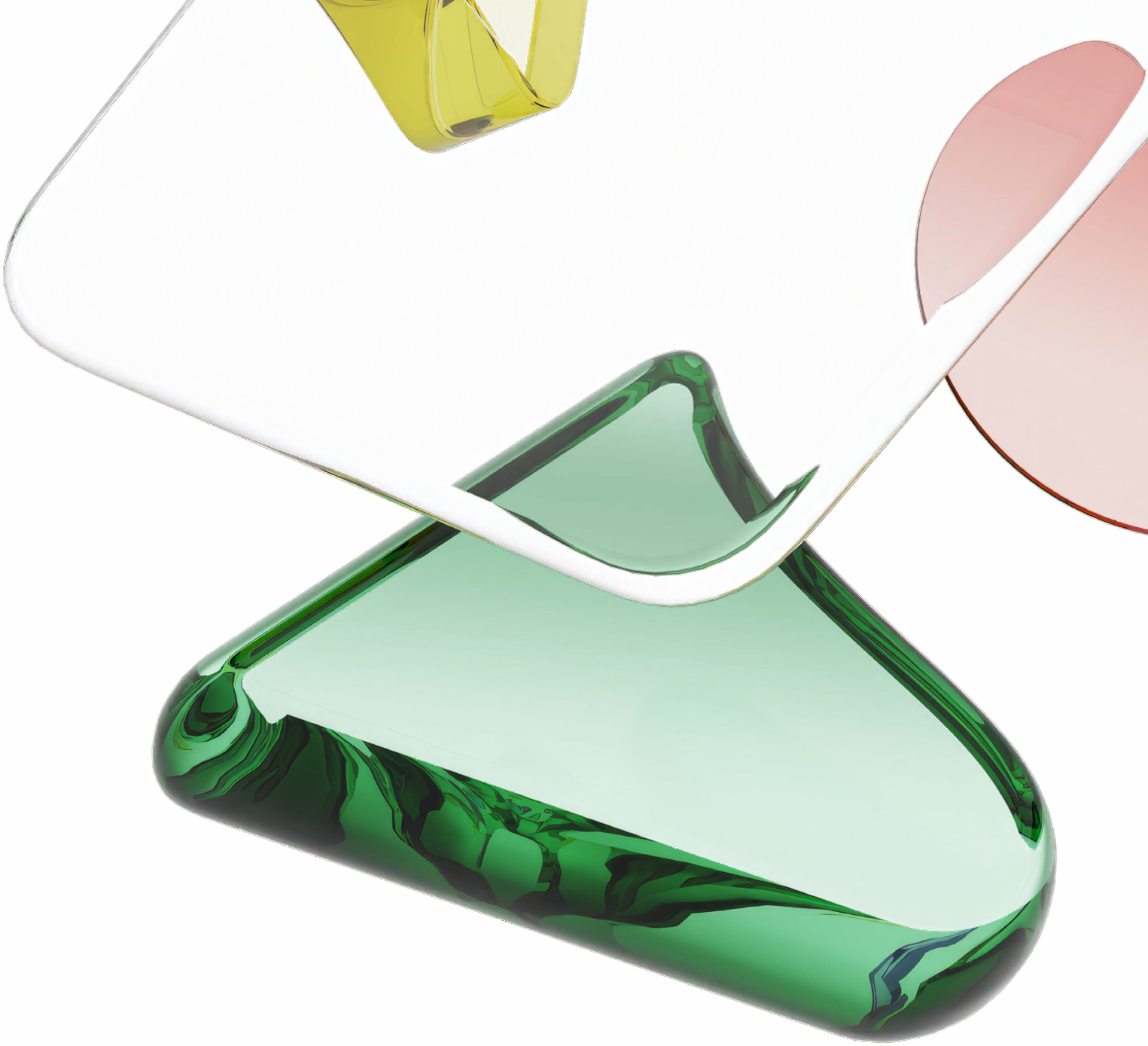
## Elevate your ISMS with ISO/IEC 27001 Certification

Based on your organization's maturity score, you may be ready to achieve ISO/IEC 27001 certification.

Certification with BSI comes with the confidence of partnering with an independent, trusted, global organization. Our expert and qualified auditors have a deep knowledge of information security management across industries, so they understand your needs and challenges.

Once you successfully complete the certification audit, BSI awards you with an accredited and internationally recognized certificate. This acknowledges your organization's commitment to driving growth, risk management, regulatory compliance and continual improvement inspiring confidence and trust in your organization from employees and external parties.

Reach out to our team to get started ›



Your partner
in progress