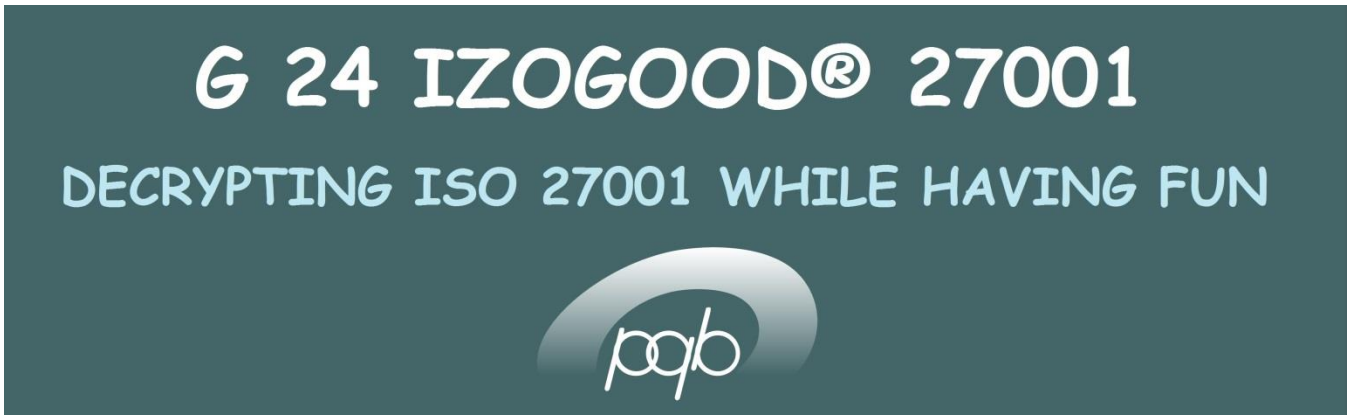

GAMER'S BOOKLET

Table of contents

1. Rules of the game

The game is intended for one person, but nothing prevents playing in a small group, it will be much more fun.

The game is compatible with recent versions of web browsers. Otherwise the game can be slow.

A game session typically lasts between half an hour to 2 – 3 hours. You can play as many times as you like during your 60-day access and learn a lot about the ISO 27001 standard.

The goal of the game is to reach the final space (Finish) as quickly as possible. 

The standard's requirements and comments are on this page. A free quiz on the ISO 27001 requirements is provided at the beginning. This allows you to discover, decrypt and become familiar with the requirements of the standard.

Having a copy of the ISO 27001 standard at hand (not provided with the game) is a prerequisite.

The board of the game is a city with a car's journey.

In the top left, there is a clock showing elapsed time. In the top right, you have a help button and option to exit the game.

At the bottom left, there's a button to mute the sound. In the bottom center, you can see the total stars you've earned. ★ At the bottom right, there's a button linking to the ISO 27001 standard requirements page.

At the beginning, the car is parked at the Start space. 

Click on the "START GAME" button to begin.

The sequence of spaces (types of cards) is as follows:

- RISK - threat or opportunity - silver
- MCT - multiple choice test - green
- PRACTICE - good or bad practice - orange
- CASE – situation, challenge and solutions - blue

You also have special Maintenance  and Pandora's box spaces  .

Each type of case includes 50 questions (cards), and each answer is linked to a paragraph of the ISO 27001 standard version 2022.

Each card is presented in the following steps:

- step 1: The back of the card showing the card type, number (from 1 to 50) and the number of stars (from one to three) in blue, white and red ★☆☆★★★

- step 2: The card type, its number, the question (e.g., “Is the following statement more of a threat or an opportunity?”), the statement (e.g., “The scope of the ISMS describes the company’s main activities”) and the star(s)
- step 3: The answers (one or more correct answers are possible) with a green emoji (for **all** correct answers)  and a red emoji (for a wrong answer) 
- step 4: The paragraph from the standard and a comment for the correct or incorrect answer

The car starts and arrives at the Risk space. 

The card number is random. Depending on the question’s difficulty, the stars are one, two or three.

If you guess the correct answer, the car moves forward as many spaces as there are stars on the question.

If you don’t guess the correct answer (or answer partially) the car stalls on the same space, and the next card will be of the same type.

If you land on a Maintenance  or Pandora's box space  , you may get lucky or unlucky. From the car’s trunk or Pandora's box comes a random luck or misfortune card. If luck is on your side, you get Joker card  , and your car moves forward 3 spaces. If misfortune strikes  , your car moves back 3 spaces.

If a second person is with you and has printed this booklet, they can increase the game’s difficulty by asking questions like:

- What is the clause and sub-clause (paragraph) of the standard related to the question?
- Can you provide an example from your department related to this question?

When you reach the Finish space for the first time, you can download your IZOGOOD® 27001 game participation Certificate. 

You can also view your game results:

- number of stars earned 
- date and time each time you played 
- time spent 

The educational objectives of the game are to allow each player to:

- identify whether a risk is more of a threat or an opportunity

- enhance their knowledge of the standard's requirements through MCTs
- guess whether a statement is a good or a bad practice
- study each proposed case's situation, challenge, and to find the right solution (one or more correct solutions are possible)
- decrypt the clauses and paragraphs of the standard and assimilate the requirements

Some questions have a touch of humor (even if the boss forgot to say it).

Relax, it's just a game. 

A bias is inevitable regarding the "correct answers" to retain, especially for RISK or PRACTICE cards.

Here's an example:

RISK 01. Is the following statement more of a threat or an opportunity? **"The most important thing is that the company's strategy was established in the past"**

One might answer that it's a threat or an opportunity, but it depends on when the strategy was defined.

If you answer that it's a threat, you're right because it's not specified when the previous strategy was developed (a year ago, 10 years ago). There's missing information. But you could answer that it's an opportunity because you think "in the past" means 2 to 3 years ago.

Thus, the presented answers and the relevance of the comments are debatable; in the end, the truth is sometimes relative.

The IZOGOOD games are created and developed with great care. Thank you in advance for communicating any potential improvement points you've identified via the link: https://www.pqbweb.eu/contact.php

2. Glossary

The beginning of wisdom is the definition of terms. Socrates

Some specific terms:

Asset: *any element of value to the organization*
Audit evidence: *demonstrably true data related to audit criteria*
Audit: *a systematic and independent survey to determine whether activities and results comply with pre-established measures and are capable of achieving the objectives*
Availability: *property of information to be usable in time (see also ISO 27000, 3.7)*
Backup: *copy of data in order to archive and protect against loss*
Competence: *personal skills, knowledge and experiences (see also ISO 9000, 3.10.4)*
Concession (after production): *written authorization to deliver a nonconforming product*
Confidentiality: *property of information accessible only to authorized persons (see also ISO 27000, 3.10)*
Conformity: *fulfillment of a specified requirement*
Continual improvement: *permanent process allowing the improvement of the global performance of the company*
Corrective action: *action to eliminate the causes of nonconformity or any other undesirable event and to prevent their recurrence*
Cryptography: *activities of codification and decoding of information*
Customer satisfaction: *top priority objective of every quality management system related to the satisfaction of customer requirements*
Customer: *anyone who receives a product*
Document: *any support allowing the treatment of information*
Effectiveness: *capacity to realize planned activities with minimum effort*
Efficiency: *financial relationship between achieved results and used resources*
External provider (supplier): *an entity that provides a product*
Incident (information security): *unwanted and unexpected event that can compromise information security (see also ISO 27000, 3.31)*
Indicator: *value of a parameter, associated with an objective, allowing the objective measure of its effectiveness*
Information security (IS): *controls to protect the confidentiality, integrity and availability of information (see also ISO 27000, 3.28)*
Information security management system (ISMS): *set of processes allowing the achievement of the information security objectives*
Inspection: *the actions of measuring, testing and examining a process, product or material to establish whether requirements are met*
Integrity: *property of information to be unaltered (see also ISO 27000, 3.36)*
IS: *information security*
ISMS: *information security management system*
Management review: *a periodic survey carried out by top management of the management system for its continual improvement*
Management system: *set of processes allowing objectives to be achieved*
Nonconformity: *non-fulfillment of a specified requirement*
Objective: *measurable goal to be achieved*
Organization (company): *a structure that satisfies a need*
Performance: *measurable and expected results of the management system*
PEST: *Political, Economic, Sociological, Technological. Analysis to identify the influence of external factors*
Process approach: *management by the processes to better satisfy customers, improve the effectiveness of all processes and increase the global efficiency*
Process: *activities which transform inputs into outputs*

Product (or service): *every result of a process or activity*
Quality management: *activities allowing the control of a company with regard to quality*
Quality objective: *quality related, measurable goal that must be achieved*
Quality: *aptitude to fulfill requirements*
Requirement: *explicit or implicit need or expectation*
Residual risk: *risk accepted (see also ISO Guide 73, 3.8.1.6)*
Review: *a survey of a file, product, process so as to verify if pre-set objectives are achieved*
Risk assessment: *risk identification, analysis and evaluation process (see also ISO Guide 73, 3.4.1)*
Risk treatment: *risk reduction activities (see also ISO Guide 73, 3.8.1)*
Risk: *likelihood of occurrence of a threat or an opportunity (see also ISO Guide 73, 1.1)*
Stakeholder: *person, group or company affected by the impacts of an organization*
Statement of applicability (SoA): *document describing the objectives and security controls*
Supplier (external provider): *an entity that provides a product (see also ISO 9000, 3.2.5)*
SWOT: *Strengths, Weaknesses, Opportunities, Threats. Tool for structuring a risk analysis*
Top management: *group or persons in charge of the company's control at the highest level*
Traceability: *the aptitude to memorize or restore all or part of a trace of executed functions*
Validation: *notice that the application of any process, product or material allows expected results to be achieved*
Verification: *the periodic inspection survey of compliance of a process, product or material*
VLAN : *Virtual Local Area Network*
Vulnerability: *weakness of an asset that could lead to unauthorized access (see also ISO 27000, 3.77)*

Remark 1: the use of ISO 27000 definitions is recommended. The most important thing is to determine a common and unequivocal vocabulary for everyone in the company.

Remark 2: a document can be presented as documented information that must be maintained (procedure  *) or retained (record*  *).*

3. RISKS 

Recurring question: Is the following statement more of a threat or an opportunity?

RISK 01 The most important thing is that the company's strategy was established in the past
Threat § 4.1 ★★★
Every three years on average, it's advisable to verify the strategy's adequacy with the company's context and the expectations and needs of stakeholders. It's a threat because the date when the strategy was developed isn't specified

RISK 02 The company's context is an element that can be considered (even if the boss forgot to mention it)
Threat § 4.1 ☆☆
This is a requirement of the standard and is unavoidable. It's one of the first tasks to carry out since the validation of the company's strategy depends on it

RISK 03 Trying to anticipate the evolution of customer expectations is a waste of time (if the boss says so)
Threat § 4.2 ★
Since the company's goal is to sustainably satisfy its customers, knowing the evolution of expectations is a key success factor for the future

RISK 04 We can try to comply with legal requirements (if the boss agrees)
Threat § 4.2 ★
We must strictly comply with legal requirements

RISK 05 The scope of the ISMS describes the main activities of the organization
Opportunity § 4.3 ☆☆
Describing the scope of the ISMS is delimiting the entities and activities concerned. Exclusions must be specified

RISK 06 In-house promotion of process mapping (the boss said to manage on our own)
Opportunity § 4.4 ★
This is an opportunity to let everyone know about process mapping. This allows everyone to situate themselves in the overall operation of the organization and in supplier customer relationships with other processes

RISK 07 Top management commitment does not contain set objectives
Threat § 5.1 ☆☆
Top management demonstrates leadership and commitment by, among other things, ensuring that an information security policy and objectives are established

RISK 08 Top management determines and updates the information security policy in line with the company's strategic direction
Opportunity § 5.2 ☆☆
Information security policy is appropriate to the company's mission (strategic direction)

RISK 09 Top management ensures that detailed descriptions of the responsibilities and authorities of the personnel concerned are assigned and communicated internally
Opportunity § 5.3 ★
When everyone knows the job description of their colleagues, things become much simpler