THE ISO 27001 "UN-CHECKLIST"

powered by PivotPoint SECURITY

Interested in a checklist to see how ready you are for an ISO 27001 certification audit?

******ABSOLUTELY MUST READ INSTRUCTIONS BEFORE COMPLETING THE CHECKLIST******

Hi, my name is Jeremy and I'm the Director of Marketing at Pivot Point Security. I've been told by every subject matter expert we have on staff **NOT** to hand organizations looking to become ISO 27001 certified a "to-do" checklist. Apparently, becoming ISO 27001 certified is a little more complicated than just checking off a few boxes.

Straight from the experts… When I asked our consultants why checklists can be harmful, this is what I heard:

Checklists enforce the wrong idea that ISO 27001 is just a set of technical controls. In reality, it's a complete management system.

Checklists will often over-estimate how close an organization is to certification; saying something like, "I checked off 8 out of 10 boxes, I must be 80% of the way to certification" can be **VERY** inaccurate.

Checklists remove the beauty of the ISO standard: ISO's flexibility and ability to fit any organization. Directly quoted from the standard, "6.2: The organization shall establish information security objectives at relevant functions and levels." Can there really be an accurate check box for a statement that requires SME & context to accurately assess?

Pretty open & shut, right? So why are we handing you a checklist?

Here's the deal…

Everyone looking to be ISO 27001 certified is searching for an "**ISO 27001 Checklist**". Ignoring what everyone wants is a bad idea (**remember, I'm the Marketing guy**) but ignoring the advice of our expert consultants is a bad idea as well…

Do you see my dilemma???

After much consideration, here is what we will do…

On the next page **(don't look yet)** there is a list of questions that will help frame your mind around how your organization is currently positioned if you were to be considered for ISO 27001 certification.

I have been warned **(and now so have you)** these questions are meant **ONLY** to help frame the ISO standard around your organization but provide **wee** … **limited**… **little**… **scant** value in telling you how close you are to certification.

There it is, the ultimate disclaimer.

If you are still interested in our "Un-Checklist", feel free to continue at **your own risk**. Either way, we'll be here wishing you and your organization all the success in the world! Whether you work with us or not, we believe **knowing you're secure** and **proving you're compliant** is important for all organizations.

The ISO 27001 "Un-Checklist"

powered by PivotPoint SECURITY

Context – *Do you know what needs to be protected?*

Have you documented: 1.) All external and internal issues that affect your ISMS, 2.) Information security stakeholders and their information security requirements, 3.) Dependencies on other organizations that must be considered when determining what needs to be protected and where?

Leadership – *Do you know management's vision?*

Can you provide evidence of leadership's vision for: 1.) What information & how information should be protected, 2.) How roles, responsibilities & authorities required for information security will be established, 3.) How the vision will be made available, communicated, maintained and understood by all parties?

Planning – *Do you have a plan to fulfill the vision?*

Have you conducted a comprehensive risk assessment that analyzed risk and determined probability of potential impacts to achieving objectives & management's vision?

Support – *Do you have the support the plan needs to be successful?*

Can you demonstrate you have the following pieces to support your plan: resources, competencies, awareness, document management process, ability to communicate the plan internally & externally?

Operation – *Have you executed your plan?*

Can you prove your plan has been executed, per the plan? Have you: 1.) Carried out operational planning and control processes, 2.) Confirmed information security risk assessments were conducted as planned, 3.) Confirmed information security risk treatment plans were documented and implemented?

Performance Evaluation – *Is your plan successful?*

Have you demonstrated: 1.) A process for management review of the ISMS, 2.) You have conducted internal audits to determine the information security management process complies with your organization's requirements, 3.) The ability to track security metrics?

Improvement – *Are you making corrective actions and continual improvements?*

Do you have corrective action plans? Are you reacting to nonconformities identifying their root causes and implementing corrective actions to ensure a consistent, improvable, effective & repeatable ISMS is in place?

Need to fill gaps to achieve ISO 27001 certification…

PivotPoint SECURITY

Where to turn

ISO 27001 Consulting
"As-A-Service"

Simplified ISO 27001 Certification + Continued Management all for a Fixed Monthly Fee

- **Reach compliance at your own pace** - Dedicated ISO 27001 expertise to ensure you have the answers, guided documentation and extended team members you need when you need them.
- **Stay on target** - PPS hosts weekly status/coordination/working meetings between your project team and our ISO 27001 experts dedicated to your project.
- **Save time and money** – Leveraging our expertise, proven processes and artifacts simplifies the process of achieving certification.
- **Ensure you meet ISO 27001 requirements** – PPS ensures your success by validating all artifacts to guarantee they fully conform with the standard.
- **Ensure 27001 is Operationalized (not just implemented)** - PPS helps build the ISMS committee and chair committee meetings.
- **Ensure you are ready for your certification audit** - PPS conducts your ISMS Internal Audit (including Corrective Action Plans & Management Review).
- **Support You Through the Audit** - PPS provides on-site support to ensure your certification audit goes off without a hitch. We have a *100% success rate* bringing clients to ISO 27001 certification.
- **Support You Post Certification** - PPS provides the ongoing operational support to ensure that you successfully maintain your certification year after year.

Call or email to schedule an appointment

609-581-4600 info@pivotpointsecurity.com

PivotPoint SECURITY

Where to turn