Aberrant Open-ISM™

LICENSE FOR USE (READ ME)

1 LICENSE INFORMATION

2 FREQUENTLY ASKED QUESTIONS (FAQ)

2.1 WHAT IS OPEN-ISM?

Open-ISM is a templatized corpus of documentation that is designed to serve as your security program's 'control standard'--e.g., documentation that describes how you comply with security controls. ISM is an initialism that stands for "Information Security Management." You may have heard of an ISMS; ISM documentation is the central component of your Information Security Management System (ISMS).

2.2 HOW DID OPEN-ISM COME ABOUT? WHY ARE YOU DOING THIS?

There are many security standards and privacy frameworks, but very little by way of ISM documentation that is publicly available. If you're starting with a security program, the task of writing hundreds of pages of documentation to map to security controls can be overwhelming. Open-ISM is designed to get you 80% of the way to a working control standard. Our documentation is battle-tested and has withstood multiple reviews by third-party auditors and registrars with flawless results.

A quality control standard is the cornerstone of a good security program. Think of controls and the control standard as a pre-flight checklist—documented processes are one of the reasons air travel is so safe. Additionally, our ISM documentation is meant to help you avoid process gaps that would inevitably result if you had to write your own control standard from scratch.

At the end of the day, we're simply trying to make it easier for companies to implement a formalized security program by demystifying the process. In aggregate we believe this helps to mitigate a national security vulnerability. Having a documented process that is audited to ensure consistency increases the quality and reliability of control compliance. Our ultimate goal is to make the internet a safer place to conduct business.

2.3 WHAT DO YOU MEAN 80% OF THE WAY? CAN'T I JUST USE THE OPEN-ISM AND BE DONE WITH IT?

The composition of your infrastructure, processes, and procedures is highly variable. As a result, it's really not possible to write a one-size-fits-all control standard that fits every organization perfectly. Open-ISM is designed to give you a strong foundation. We give you a starting point and allow you, or a consultant, to modify the documentation to fit your organization. Think of the Open-ISM as an off-the-rack suit that requires tailoring—you or your security consultant is the tailor.

2.4 WHAT SECURITY STANDARDS DOES THE OPEN-ISM SUPPORT?

Open-ISM is explicitly designed to support CIS V8 Controls, but it has also been used by companies that support ISO 27001:2013, SSAE 18 SOC 2, CMMC, NIST 800-171, and HITRUST. Open-ISM will support any security standard or privacy framework to some degree. It should be noted that Open-ISM currently makes no mention of patient health information (PHI)—although there is a strong overlap between personally identifiable information (PII) and PHI, they are not the same. Open-ISM requires more modification for complicated standards like HITRUST or PCI DSS, but it will still save you substantial time and effort than if you had to start the process of writing documentation from scratch.

2.5 CAN I SUPPORT MULTIPLE SECURITY STANDARDS AND PRIVACY FRAMEWORKS WITH OPEN-ISM?

Yes. A control standard can support one or more security standards or privacy frameworks. In instances where you have to support more than one security standard, you should consider using common controls with a cross-walk framework.

2.6 IS IT FREE?

It depends on your use case. If you can use the Open-ISM freely if you are using it for non-commercial use—this applies to 501(c)(3) organizations as well as educational institutions. The Open-ISM can also be acquired for free depending on your membership type with Aberrant.

2.7 I'M A SECURITY CONSULTANT. CAN I USE OPEN-ISM WITH MY CLIENTS?

Yes, however, your customers in some cases may need to purchase the Open-ISM depending on their membership type. Customers that use the Open-ISM for non-commercial purposes can use the documentation free of charge. That said, you can write your own ISM documentation and use that in lieu of the Open-ISM.

2.8 DOES OPEN-ISM SUPPORT STATE REGULATIONS LIKE MA 201 CMR 17.00 OR DFS 23 NYCRR 500?

Open-ISM paired with a security standard will put you in compliance with state regulations, however, there may be specific reporting requirements in the event of a breach incident. You'll want to review legislation and augment your ISM documentation accordingly.

2.9 CAN I USE OPEN-ISM TO COMPLY WITH GDPR OR CALIFORNIA'S CCPA / CPRA?

Yes, privacy is a new and emerging area that overlaps tightly with security. It's a best practice to use your control standard to manage privacy, however, this may result in your newly minted Chief Privacy Owner (CPO) owning a portion of your company control standard. Check out ISO 27701:2019 and the NIST Privacy Framework for controls that you'll need to add to your program that will put you in privacy compliance.

2.10 WHAT ABOUT HIPAA / HITECH, SARBANES-OXLEY SECTION 404, GLBA, FEDRAMP, ETC.

It's important not to conflate laws and regulations with security standards. Security standards are controls that put you in compliance with laws and regulations. Open-ISM supports all security standards, albeit to varying degrees.

2.11 DO I NEED ALL THE DOCUMENTS IN THE OPEN-ISM? THERE ARE A LOT OF DOCUMENTS!

You probably don’t, some of the documentation will be superfluous to you. For example, if you don't have a physical office the Physical Security Policy can be deleted since any physical security controls will be out of scope for your program.

2.12 WHAT’S MISSING FROM THE OPEN-ISM? DOES OPEN-ISM CONTAIN ALL THE DOCUMENTS THAT I’LL EVER NEED?

If your company grows larger, you’ll likely want to add additional policies and procedures. Here are some examples of documents that you’ll likely want to add:

- Enterprise Architecture Governance policy
- Internal SLO procedure
- Software Acceptance policy/procedure (NIST 500-180)
- Red Team Policy

You may also need to add additional documentation to comply with security standards like SSAE 18 SOC 2: e.g. an “SSAE 18 SOC 2 Report Addendum.”

2.13 DOES THE OPEN-ISM ADDRESS PROGRAM GOVERNANCE?

Yes, we think including governance in your security program design is a best practice. Governance defines things like approval workflow. That said if you disagree you are free to eliminate the governance documentation. It should be noted Governance is superfluous to the CIS V8 Controls standard, but we still think it’s a good idea that you include it.

2.14 WHAT’S THE DIFFERENCE BETWEEN A STANDARD, A POLICY, AND A PROCEDURE?

The term standard is overloaded in the security space. We define the control standard as, “a set of company approved policies and procedures that describe the company’s security program. Technically, there should only ever be one control standard per security program. The rule is one security program has only one control standard.”

Governance documents are sometimes referred to as standards because they apply to the control standard generally—e.g. the ISMS Document and Records Control Standard.
A policy is a document that requires formal approval by a governing committee. Policies are directives and are generally devoid of information related to implementation.

A procedure is more of a ‘how to’ document and requires less formality to update—procedures contain implementation detail. If your program does not include governance then this distinction likely isn’t important to you. As your security program gets bigger this distinction may become relevant to you. It should also be noted that federal auditors of regulated entities are more likely to want to review your policies than your procedures.

That said, you’re free to rename documents if you need to.

2.15 WHY ARE THE CONTRACT DOCUMENTS BLANK?

We add placeholder documents for legal documents that you'll want to have. You might want to consider having your legal counsel draft up an NDA, LOI, Terms of Use, and MSA for your company. The documents that your company needs really depend on your business.

2.16 WHAT IF I HAVE RECOMMENDATIONS OR SUGGESTIONS? WHOM DO I CONTACT?

Please contact info@abberant.io. Your help with making our documentation better is always welcome!