Selecting the Right Policy Set

February 2017

CONTENTS

EXECUTIVE SUMMARY

There are only 4 Foundations of Security. Regardless of your business's size, region, or industry sector, unless you have the following in place your security program will fail:

1. **Management Buy-In / Culture** - The vast majority of the responsibility for the security culture of any organisation falls firmly on the shoulders of the CEO (or equivalent).

Unless your company IS a security company of some sort, security is an expense, and whether or not that expense is seen as a business enabler (which it is) depends on the CEO's attitude towards it.

The remaining foundations have little chance of success unless you get this one right.

2. **Policies & Procedures** - It's amazing how many people groan at this, and even security professionals cringe at the 'paperwork' they have to troll through.

That's a shame really, because without that paperwork, you will never HAVE security. It's your company's instruction manual for how to do what you do, properly, responsibly, and *securely.* Anyone who's put together a chest of drawers from Ikea knows exactly what I mean; maybe, and I mean MAYBE, you could work it out for yourself, but how much more painful would that be? It's bad enough WITH the instructions!

Your policies and procedures let all employees know what to do, and as importantly, what NOT to do. It's enough that the thieves want to steal your data, why make things worse by not preventing your own employees from giving it away!?

3. **Governance** - Few phrases in security are perceived to be more ambiguous, open to interpretation, or complicated.

Wikipedia says; "*Information Technology Governance is a subset discipline of corporate governance focused on information technology (IT) systems and their performance and risk management.*"

I can simplify this to; "IT Governance is the business side and the IT side having *meaningful* conversations."

It does not have to be complicated, it just has to be appropriate. You don't have to hire additional people to run it, you just have to assign the tasks, responsibilities, and accountability.

4. **Education & Training** – Self-explanatory, I hope.

The Policies are arguably the most important of the 4, as without them, there can *be* no foundation on which to build the remaining program.

ADDRESSING THE CHALLENGE

First, you must define each of the document types you are creating:

- **"Policy"**: Organisation-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures. In other words the DOS and DO NOTS of expected behaviour. Typically consist of language like; must and must not, shall and shall not etc. Contents are mandatory.
- **"Standard"**: Specific requirements and parameters of operation for the organisation. Standards define *exactly* what something must look like. From operating systems, to network devices, to application & software, this is how they will be configured.
- **"Procedure"**: Descriptive narrative for a Policy. Procedure is the "how to" for a Policy and describes how the Policy is to be implemented. Often, Procedures will be step-by-step instructions on how to perform a specific action. As such they represent the sum of almost all corporate knowledge as it relates to the running of a security program.
- **"Guidelines"**: A non-mandatory good practice, often use to help less experienced individuals meet the intent of the above documents.

Second, you need someone to run the project internally (a Policy Coordinator), and likely an external consultant to provide the necessary expertise to ensure the Policy Set stays appropriate to the business culture and goals. If regulatory compliance is a big driver, you will need to choose a consultant with sufficient expertise.

Third, you must define the documents required. Up front. If you already have some documentation, you'll only be looking to fill the gaps. But if you're starting from scratch, you need to choose a Policy Set of *appropriate* depth and breadth. Most vendor supplied Policy Sets are designed with large business in mind, meaning the vast majority of the content will need to be adjusted or even removed altogether.

Fourth, define how the resulting Policy Set will be managed moving forward.

- Do you have an Intranet on which these documents can be distributed?
- Would a Document Management System (DMS) make more sense?
- Do you have an online training platform that can be used to not only distribute the Policy Set, but train employees in their use?
- Can HR add these documents to both the on-boarding process and the ongoing awareness training curriculum?

And lastly, distribute the ongoing review and maintenance of every document to the role best qualified to do so. If you have a IT governance function, add the Policy to their list of responsibilities.

WHAT'S IN A POLICY SET?

Depending on the size and complexity of an organisation, there can be a few dozen to several hundred documents. However, the following *should* be part of every Policy Set regardless of organisation size, region, or function:

Mandatory Polices[1]

- ***Information Security Policy Framework (ISPF)***: The ISPF is the overarching document of the Policy Set and sets the tone for everything that comes after it. The most important sections will include:
    - *IS Role & Responsibilities* - Who is supposed to do what, from the CEO down to the most junior employee;
    - *Documentation Development* - Makes the Policy Set mandatory;
    - *Policy Format / Naming Conventions* - Standardises all Policy Set content;
    - *Policy Exceptions* - There will always be times when you cannot perform something in-line with your polices, but this must be approved and tracked accordingly; and
    - *Change Management* - Makes change control mandatory
- ***Acceptable Use Policy (AUP)***: Not every policy is appropriate to distribute to every employee, but there are some things that must be enforced across the board. The AUP - often called the Code of Conduct (CoC) – sets out those things that are to be followed by everyone, form the Board of Directors (BoD) to external consultants.
  The AUP End User Agreement is signed by every employee and a copy of that signature must be held on file.
- ***Data Classification Policy***: No Policy Set is complete without data classification, as every other policy will in some way refer to it, and / or be labelled *with* its contents. There can be no 'appropriateness' in security until you've baselined your controls to the risk of loss.
- ***Business Continuity Policy***: Not much point being in business if you don't make *staying* in business a mandatory requirement.
- ***Risk Management Policy***: This can include everything from mandatory risk assessments, to incident response and disaster recovery. Regardless of what it contains, the risk management policy requires the organisation to measure its risk in a standardised fashion and mitigate that risk appropriately.

[1] *Note: Lists of the most common Polices can be found at Annex A*

Mandatory Standards[2]

- ***Document Management Standard:*** From numbering, to style/format, to content, what goes into a document must be fully defined.
- ***Asset Registration Standard:*** Asset management is the centre of every security process. From risk assessments, to vulnerability management, if you don't know what you've got, you can't protect it.
- ***Configuration Standard(s):*** Every asset must be installed in a manner that supports one of the tenets of security; least privilege. Configuration standards are the only way to ensure that security in built in from the beginning, and how security is maintain throughout an asset's entire life cycle.
- ***Authentication Standard:*** You will refer to 'strong authentication' throughout all other documents in the policy set, this is where you define what it means.
- ***Vulnerability Management Standard***: The word 'periodic' has no place in standards, so everything you have to do for vulnerability management (patching, scanning, penetration testing etc.) must have a definitive schedule.

Mandatory Procedures

- ***Document Management Procedure***: How the Policy Set is to be managed and maintained.
- ***Change Control Procedure***: Nothing in an organisation should change without explicit permission. How that change is effected without creating a bottleneck and who can approve changes is defined in this procedure.
- ***Policy Exception Procedure***: In reality it is impossible to conduct a business within the confines of the policy statements. However, that is no reason for performing any action outside of the *scope* of a Policy Set. The exception process is the official way to continue performing a function with full oversight into the risk of doing so.
- ***Incident Response Procedure***: No point being in business if you don't intend *staying* in business. Robust incident response procedures are about the only way you can prevent a security event - which *will* occur - into a business crippling disaster.
- ***Disaster Recovery Procedure***: Inevitably, things will go wrong. Organisations that can get back on their feet faster stand a better change of fully recovering. This procedure, or more likely procedures, should fully define how to get every business process back online.
- ***Security Training & Awareness Procedure***: What must everyone in your organisation know in order to fully support / enable the business goals? As one of the 4 Foundations of Security a well-defined procedure is critical the success of any security program.

[2] *Note: Lists of the most common Standards and Procedures can be found at Annex A*

ASK FOR WHAT YOU NEED

The questions below are designed to be generic enough to suit almost any business, as well as form the core questions in your Request for Information / Proposal (RFI / RFP);

1. *On which information security framework or frameworks is the Policy Set based*

   Regardless of the reason you require a Policy Set - to achieve Payment Card Industry (PCI) compliance for example - your policies should be based on an industry acceptable framework for the management of a security program. There are several; Control Objectives for Information and Related Technology (COBIT), NIST SP 800 Series etc., but it's the ISO 27000 Series that has been dominant globally for much of the last decade.

   Other than PCI, no other regulatory compliance regime on the planet that we have seen makes any of these frameworks mandatory, but it just make sense to choose the most common and map your policy set to it. Many organisations have mapped the other frameworks to ISO 27001, so it should be a simple process to obtain these if required. Whatever your requirement, make sure you choose a policy set that meets not only your immediate compliance needs, but the needs of your business across the whole relevant regulatory landscape.

2. *Can you provide a list of included policies?*

   No policy set can ever include completed Standards or Procedures, these are entirely unique to an organisation, but the Policies should cover just about any business with a little customisation. Assuming the Policies have been mapped to an appropriate framework, deciding how the Polices should be amended should be very straightforward.

   The better policy sets will include every policy statement an organisation could possible need, along with the context for its inclusion or exclusion.

3. *Does your service include a mapping of policy statements to the PCI DSS?*

   While this question seems to be a little specific, no other compliance regulation in history has driven the need for commercially available policy sets quite like PCI. It therefore makes sense that, at a minimum, all relevant policy statements are mapped to the PCI DSS out of the box.

   Ideally, there will be three mappings based on the latest version of the PCI DSS:

   i. All policy statements mapped to the PCI DSS (as stated above);
   ii. The PCI DSS mapped to all policy statements as well as all Standard / Procedure templates; and
   iii. The PCI DSS Report on Compliance template mapped to all policy set templates.

   Compliance with PCI is almost 40% 'paperwork', if you're going to invest in a Policy Set you want this work done for you.

4. *Does your service include a mapping of policy statements to ISO27001 (or whatever Information Security framework you used)?*

   Similar to the PCI question above, there's little point in purchasing a policy set if it's not already mapped to the framework upon which you have based, or will be basing, your entire security program.

   Only an appropriate mapping of the policy statements to your chosen framework allows you to determine the impact of your customisation process. You must have this appropriate context or your policy set may not support your regulatory compliance efforts.

5. *Can you provide a Document Management Standard and Procedure?*

   One of the biggest drawbacks of buying a policy set is that few people have the necessary skill-set to maintain it once the vendor has completed the initial customisation. Policies, Standards and Procedures must be constantly reviewed for validity, amended in response to internal and external influences, and distributed to everyone with a need to know.

   Well-documented management standards and procedures allow organisations to keep their policy set relevant, and if required, compliant. No organisation should ever rely on a 3rd party to maintain their paperwork (see Question 12).

6. *Do you provide an Information Security Governance Charter template?*

   The word 'Governance' is usually enough to put organisations off altogether. Surely only large organisations need something so 'official'? Nothing could be further from the truth. IS Governance is where the business side and the IT have meaningful conversations about how to achieve the business's goals. It is therefore perfectly placed to be responsible for the policy set. The challenge for most organisations is where to start.

   A well-written and appropriate Governance Charter is often all organisations need to overcome their inertia, whatever the cause.

7. *Do you provide document templates for the most common Procedures and Standards?*

   Any vendor offering a Policy Set that includes drafts of every Standard and Procedure is often nothing more than snake oil. Both Standards and Procedures are totally unique to each organisation, and can never be entirely relevant out of the box.

   That said, every document in a policy set has standardised content headings; e.g. 'Objective' / 'Scope' / 'Document Management' etc. These templates can all be drafted based on most common content and established usage. The most any vendor can provide are templates for all the most common Standards and Procedures, as well as examples of the ones a little more difficult for the inexperienced to understand (see Question 8).

8. *Can you provide best practice samples of the more common procedure / standard documents?*

   Per Question 7. above, only the Policies can truly contain relevant content out of the box. However, there are several procedures where client specifics will be built on a standard framework.

   For example, the following Procedures are all predicated on a chosen best practice framework:

   i. Document Management Procedure
   ii. Risk Assessment Procedure
   iii. Incident Response Procedure

   So while the full specifics will be customised to the individual organisation, the guidance related to these more difficult concepts in the form of examples can be invaluable.

9. *Do you include an instruction manual to enable self-customisation?*

   Many commercially available policy sets are based on Microsoft Word templates. While there is nothing wrong with that, few come with an instruction manual on how to customise them to meet your existing brand requirements.

   This gap often forces organisation to purchase additional consulting time to perform this relatively simple task, so the better Policy Sets will include a manual to allow you to customise the entire thing yourself.

   There are online versions of the policy set service, but you will need to be very careful in choosing one of these options as internal distribution of the results can be troublesome. Again, you must define your needs first, then choose the right option for you.

10. *Can you scale your consultancy offering to include a fully bespoke Policy Set?*

    The development of a policy set may be relatively simple to those already with the skill-set, but it can look extremely complicated to a non-security expert. There is therefore little point in a vendor offering a policy set without having the necessary consulting skill-sets backing them up to actually deliver a final product.

    However, this service should be entirely scalable and bespoke to each organisation's needs. If all that is required is a few polices to fill the gaps in existing documentation, then the consulting service should adapt. If an organisation requires every document from scratch, then the service must include a significant level of guidance to enable self-sufficiency when the consultant is through.

11. *Do you provide your policy set in other languages?*

    The vast majority of vendors will only provide policy sets in English, so if you have language requirements you must ask up front. And get samples, Google Translate will not get the job done.

The alternative is a translation service. It's possible a vendor has existing relationships to get this done cheaper, but you should still do your own homework.

12. *Can you help us manage this moving forward?*

    As stated previously, no policy set service should involve an ongoing relationship that includes maintaining the entire documentation management program. You don't brush your children's teeth every day, you teach them how to do it for themselves.

    That said both the prevailing threat landscape and the regulatory landscape are in constant flux. Therefore, vendors offering an ongoing advisory service, even under a paid retainer, are providing a more sustainable offering.

13. *What if we fail to achieve compliance with our chosen regulation?*

    No policy set vendor can guarantee compliance first time around. Compliance with any regulation is almost entirely predicated on the interpretation of an auditor/assessor, each with their own unique biases.

    However, if you write the achievement of compliance into the contract as an SLA, you can ensure that the vendor makes the necessary adjustments per the assessor's findings. At least for the Policies.

14. *Monolithic vs. Modular*

    While this is largely a matter of preference, monolithic policy sets tend to be extremely difficult to manage. Assigning ownership to a document section, as well as recording version history, are next to impossible unless each subject is a stand-alone document.

    Distribution and awareness also become an issue when the vast majority of a monolithic security policy's content is irrelevant to most employees.

    It is also my experience that most monolithic policies were written to scrape through soe kind of compliance requirement, PCI being the most common offender. If a policy set is only seen in this light you may as well get the cheapest.

15. *How long does the process take?*

    Basically a trick question, there are way too many dependencies on the client side for any vendor to estimate how long the service will take. However, any additional consultancy should be valid for at least 1 full year as that's how long it could take to get the program in place. Assuming of course that it's implemented correctly.

SUMMARY

Choosing a policy set can seem complicated at first, especially if you do not have a security specialist on staff. However, if you keep the following points in mind, and ask all the questions above, you should be able to choose the right policy set for your business goals, whatever they may be;

1. At a bare minimum, get the CEO to sign the ISPF. If you can't get him/her to accept the accountability for security in this limited fashion the rest of the program will be seen as nothing more than a burden;
2. Policies must be a reflection of your existing corporate culture, not a radical shift in response to some external compliance requirement;
3. Policies should always be aspirational in nature, otherwise continuous improvement is next to impossible;
4. As a corollary to 3., use the exception process to record everything you are NOT doing relevant to your policies. These are the first entries onto your risk register;
5. Assign all Policies to the highest level and to the most appropriate role in your organisation. While these individuals may not actually write the content, they should be fully accountable for its distribution and enforcement;
6. Assign coordination of all Standards and Procedures to the SME most suited to do so; and
7. Work closely with an independent body (Internal Audit or outsourced equivalent) to ensure that the policies are appropriately enforced.

In the end, choosing the right policy set is dependent on why you're buying one in the first place. If it's just for PCI compliance only, then you might as well by the cheapest and crappiest offering out there, nothing will help you be secure.

If, however, you actually care about security, *and* recognise the enormous benefit a good security program can bring to the business, then you really need to do your homework.

No, it will not be cheap, but you'll get what you pay for.

Best of luck!

ABOUT FROUD

David has almost 20 years of experience in areas of Information / Cybersecurity, including Regulatory Compliance, Secure Architecture Design, Governance Frameworks, Data Privacy & Protection, and FinTech.

As Project Lead for several Fortune / FTSE 'Enterprise Class' clients, David has performed hundreds of on-site PCI, security, and regulatory compliance assessments for organisations globally.

Blog: http://www.davidfroud.com

Linkedin: http://www.linkedin.com/in/davidfroud

ABOUT CORE CONCEPT SECURITY

Core Concept Security (CCS) is an independent cybersecurity and data protection consulting practice based in the UK, but available globally.

The guiding principle behind all CCS's services is that security, while often difficult to achieve, has always been, and will always be, simple. There are no shortcuts to security, and there is nothing to be gained by just throwing money at it hoping the problems will go away. Technology will never fix what's broken, only people and process can.

The CCS approach is also simple; It's our job to help you ask the right questions, even if we aren't the ones who can actually answer them. You're hiring us, you're hiring everyone we know.

In the end, if your security program is not appropriate to your business needs it is a waste of your time and effort. Our commitment to our customers is to never settle for less than, or try to sell you anything *more* than, what you need.

ANNEX A – MOST COMMON POLICY SET DOCUMENTS

Policies:

- Information Security Policy Framework
- Acceptable Use Policy
- Acceptable Use Policy-End User Agreement
- Data Classification Policy
- Data Handling & Media Destruction Policy
- Data Retention and Role Access Policy
- Asset Management Policy
- Business Continuity Management Policy
- Access Control Policy
- Remote Access Policy
- Risk Management Policy
- Incident Response Policy
- Disaster Recovery Policy
- Vulnerability Management Policy
- Security Awareness & Training Policy
- Cryptography & Key Management Policy
- System Configuration & Maintenance Policy
- Network Configuration Policy
- Secure Application Development Policy
- Use of Critical Technologies Policy
- Vendor Management & Due Diligence Policy
- Telecommuting & Mobile Computing Policy
- Physical Security Policy
- Privacy & Regulatory Compliance Policy

Standards:

- IS Document Management Standard
- [DESKTOP-LAPTOP] Configuration Standard
- [FIREWALL-ROUTER] Configuration Standard
- [IDS-IPS] Configuration Standard
- [OPERATING SYSTEM] Configuration Standard
- [WIRELESS ACCESS POINT] Configuration Standard
- Asset Registration Standard
- Authentication Standard
- Logging & Monitoring Standard

- Penetration Testing Standard
- Software Development Life Cycle
- [PHYSICAL SECURITY] Standard
- Encryption & Key Management Standard
- Network Time Synch Standard

Procedures:

- IS Document Management Procedure
- Change Control Procedure
- Data Backup & Media Handling Procedure
- Data Destruction Procedure
- Encryption & Key Management Procedure
- Firewall-Router Change Request Procedure
- Incident Response Procedure
- Log Review & Monitoring Procedure
- Disaster Recovery Procedure
- Periodic Security Operations Procedure
- Risk Assessment Procedure
- Rogue Device Detection Procedure
- Security Awareness Training Procedure
- User Access Request Procedure
- Vulnerability Management Procedure
- Vendor Due Diligence Procedure
- Policy Exception Procedure
- Asset Registration Procedure
- Software Approval Procedure

Other:

- New Policy Template
- New Procedure Template
- New Standard Template
- Governance Steering Committee Charter
- Master Document Register
- Policy Master & Compliance Mapping
- Document Template User Guide