Accelerated Risk Management (ARM)

The Universe of InfoSec Risks Assessed in Minutes, Not Days
THE RISK ASSESSMENT DILEMMA:

Risk Assessment is the foundation of Information Security management and required by virtually every standard

+ Comprehensive Risk Assessments require significant time & expertise, so they are not executed often or optimally

= Without understanding risk you can easily implement the wrong controls, to the wrong maturity level (all at considerable expense), and still leave yourself at risk
Risk Management Is CHALLENGING

Risk Assessment Requires Time
Comprehensive identification of information related risk & thorough analysis of those risks to determine if they are currently managed to an acceptable manner; requires notable time investment.

Risk Assessment Takes Expertise
Developing a risk management framework and then applying it across diverse technical, business, & product environments requires a rare level of experience & expertise.

Risk Assessment Takes Diligence
As laws, contracts, clients, threats, & technology evolves, so too does your Risk; If you are not assessing risk frequently, you are at risk.

Risk Assessment is Subjective
When all you have is a hammer, everything looks like a nail. Security expertise, experience, client expectation, schedule, & industry expertise result in your risk telescope focusing on certain galaxies of risk, and entirely missing others, in your risk universe.
Pivot Point Security has helped thousands of companies manage their “universe of risk” over the last 20 years.

This is what we do.
Our Accelerated Risk Management (ARM) expert system is a paradigm shift in Risk Assessment.

You Don't Need to Continue Down The Same (Expensive, Time Consuming, Modest Quality) Path
How ARM Simplifies Risk Management

Perform Risk Assessments in Far Less Time & With Less Team
Comprehensive automated identification & analysis of information related risk & suggestions on additional risk mitigation happen "auto-magically".

Leverage Your Business Expertise
Leveraging our expert system for Risk Analysis lets you be successful without deep information security risk assessment expertise.

Automation Encourages Diligence
When updating your Risk Assessment is measured in minutes instead of days, it becomes habit, like putting on your seat belt.

Objectivity Trumps Subjectivity
Automation isn't subjective; ARM moves Risk Assessment from Art to Science, so that your risk universe is well explored (to infinity & beyond!!)
We Have A Proven Process for a Risk Assessment (RA), that is fully completed in hours

- **Monday, 3 PM**
  - Step #1: Generate an inherent RA based on your scope (information & requirements)

- **Tuesday, 10 AM**
  - Step #2: Generate a questionnaire to understand current infosec control maturity
  - Step #3: Import the answered questionnaire to determine residual risk
  - Step #4: Tune recommendations for risks that are not yet at an acceptable level
Step #1: Each Organization's Risk Is Different ...

ARM accounts for those differences

1. Different quantities & types of data they process
2. Different laws, frameworks, technology that apply to that data (e.g., Cloud, CCPA, IoT, PHI)
3. Different risk acceptance criteria
4. Different levels of impact to a risk being realized
5. So ARM generates an inherent risk assessment that is unique to these “data points” that it is provided...
Step #2: ARM Creates Questionnaires That Perfectly Match Inherent Risk/Regulations/Tech

Check out these examples

If Personal Health Information is being processed ARM will ensure the questionnaire addresses HIPAA

If Personal Information is being processed ARM will ensure the questionnaire addresses what is applicable to you (CCPA, GDPR, 27701)

If there is extensive use of the Cloud or IoT, ARM will ensure the questionnaire addresses Cloud & Embedded Device Requirements
Step #3: ARM Uses the Maturity of Each Control to Calculate Your Residual Risk

- Each controls' 0-5 CMM score is used to determine how much it mitigates each risk identified.
- ARM compares the remaining (residual) risk to the acceptable risk you specified.
- ARM determines the optimal improvements to controls necessary to mitigate any risks which are not yet acceptable.
### Step #4: Auto Generate Reports

- **Limited visibility and control over Shadow IT**
  - License management is informal and may result in unauthorized software or unused licenses.
  - Mitigate: Increase **IAO-04** (Threat Analysis & Plan Remediation During Development) from Planned & Tracked (2/5) to Continuously Improving (5/5).
  - Enable administrator role for installation of unapproved software.

- **Vulnerable Internet of Things (IoT) or Operational Technology (OT) device**
  - There is no formal methodology regarding information security requirements gathering or security testing for internal applications.
  - Mitigate: Increase **TDI-15** (Threat Detection Analysis & Fix) from Quantitatively Controlled (4/5) to Continuously Improving (5/5).
  - Implement an MFA solution.

- **Vulnerable teleworker (home computer, mobile workforce, travelling employees)**
  - There is currently no laptop travel policy.
  - Mitigate: Increase **AST-04** (Network Diagrams & Data Flow Diagrams (DFD)) from Well Defined (3/5) to Continuously Improving (5/5) and increase **DFD-01** (Standardized Operating Procedures (SOP)) from Planned & Tracked (2/5) to Continuously Improving (5/5) and increase **GROUP-02** (Publishing Security Policies) from Well Defined (3/5) to Continuously Improving (5/5). 
  - Define procedures for going offsite when traveling outside of our environment.

- **Poor password management practices (mobile, cloud, network, applications, sharing)**
  - Some servers and applications rely on legacy systems where the passwords have not been changed for several years.
  - Mitigate: Increase **IAO-03** (System Security Plans (SSP)) from Well Defined (3/5) to Continuously Improving (5/5) and increase **IAO-04** (Threat Analysis & Plan Remediation During Development) from Planned & Tracked (2/5) to Quantitatively Controlled (4/5).
  - Ensure that systems that password configurations are modified or replaced.

- **Inconsistent infosecurity business continuity**
  - Backup restoration testing is not always conducted monthly.
  - Mitigate: Increase **IAO-04** (Threat Analysis & Plan Remediation During Development) from Planned & Tracked (2/5) to Continuously Improving (5/5) and increase **IAO-03** (System Security Plans (SSP)) from Planned & Tracked (2/5) to Continuously Improving (5/5).
  - Ensure that backup procedures are documented and tested at least annually.

Where necessary, ARM suggests improvements for any risk which is not yet acceptable (e.g., “Improve the control System Hardening Through Baseline Configurations (CFG-02) from its current maturity of 2.0 to at least 3.0 (per the provided maturity guidelines).”)
Accelerated Risk Management (ARM)

Break the Law of Constraints

Faster
Automated Risk Management can be completed in hours not days

Better
Repeatable, contextualized, comprehensive, objective, accurate

Cheaper
Time is money & risks not realized are losses not realized (& yes our marketing guy wasn’t happy with our use of the word cheap :>))
Other Benefits of ARM

There's more to love ...

1. ARM demonstrates to stakeholders that EVERY risk was considered (conventional RAs show what was analyzed but not what wasn't)

2. ARM includes a documented Risk Methodology which you need for certification for standards like ISO 27001

3. RAs are easier & faster, so, you do them more often so you experience notable reduction of your risk

4. Repeatable and consistent independent of the person or team that conducts the RA
You can continue to grind through your Risk Assessments, or...
You can accelerate through reviews with ARM from Pivot Point Security
FAQ's, because ...

ARM is a Paradigm Shift

Come on... you must have more questions!

[Image of a user interface with tables and dropdown menus]
Frequently Asked Questions

• How Does ARM Work?
ARM is an expert system with a predefined library of vulnerabilities and threats. ARM is able to accurately quantify the likelihood and impact of EVERY threat acting on EVERY vulnerability for EVERY data type you process. It literally calculates every potential risk in your Risk Universe.

• Has ARM been validated?
ARM has been through dozens of successful ISO-27001, SOC 2, HIPAA, NIST, & SEC audits. It fully meets the requirements of major Risk Management Frameworks like ISO-27005 & NIST SP 800-30.

• How does ARM compare to other Risk Methodologies?
Like OCTAVE, FAIR, IRAM, 800-30, and ISO 27005 ARM applies a standardized model to Risk Analysis; it takes an automated, information (not asset) centric approach.

• Is ARM Qualitative or Quantitative?
ARM provides both a Qualitative (Low/Medium/High) and semi-quantitative (0 - 100) mechanism to analyze risk (we prefer the latter as it provides greater granularity in risk management decisions).
Frequently Asked Questions

- **What is Inherent Risk?**
  
  Inherent Risk = Business Impact of Threat Exploiting a Vulnerability * Probability of that occurring (for each data type you assess you will add the impact)

- **What is Residual Risk?**
  
  Residual Risk = Inherent Risk – Remediation for Current Controls implemented that reduce that risk; ARM adjusts the amount of remediation based on the maturity of each control

- **Does ARM support X standard?**
  
  ARM considers 800 controls across 125+ security & privacy standards (ISO 27001, SOC 2, HIPAA, NIST 800-171, CMMC, PCI, FFIEC, etc.)

- **What file format does ARM use?**
  
  ARM generates all questionnaires and risk assessments in Excel to make them as easy to use as possible
Frequently Asked Questions

• How is ARM offered?
PPS offers ARM as a managed service (consultant supported) & will soon offer ARM in a SAAS model & as a JSON API for tool integration

• Is ARM Secure?
ARM runs in AWS and is ISO-27001 certified. More importantly, ARM doesn't store your data

• Is ARM proven?
PPS has used ARM as an internal service offering for 100+ risk assessments over the last 2 years

• How do we “interact” with ARM?
Via acceleratedriskmanagement.com you will enter the required inputs (data types, impacts, regulations, & acceptable risk), generate your questionnaires/assessments, & upload your completed questionnaires