A PRACTICAL APPROACH TO SUFFICIENT INFOSEC

Dr. Rayford B. Vaughn, Jr.
Mississippi State University
Department of Computer Science
PO Box 9637
Mississippi State, MS 39762
(601) 325-2756 fax (601) 325-8997
vaughn@cs.msstate.edu

[*This paper examines an approach to information which is based on providing the customer with "Sufficient INFOSEC" based on needs as determined through a process that includes a business review, risk analysis, engineered solutions, and continuous review. It recognizes the absence of absolute security in any practical sense and promotes "adequate" security based on assurance based risk mitigation. It promotes the idea that security protection needs are dynamic – not static, and environmentally driven. A secondary issue is raised in questioning the lack of flexibility present today in DoD with respect to INFOSEC regulations that fail to take into account the environment being protected*.]

KEYWORDS: Computer Security, INFOSEC, Security, COMPUSEC, Risk Assessment

1. INTRODUCTION

1.1 OVERVIEW

The concern with securing Department of Defense (DoD) systems and the numerous electronic repositories associated with these systems has been an active endeavor and subject of significant research effort since the mid-60's. The research conducted has not been without result, and over the past 30 years DoD has taken the lead in providing processes, understanding, and products to assist in reducing the risk of information compromise, loss of integrity, or its non-availability. This is evident when one reviews the literature and DoD guidance published via the "Orange Book" [1] and its associated "Rainbow Series" beginning in the mid-80's and continuing today. These efforts are not often recognized for the foundation work they have provided to the automation and networking community as a whole, but are certainly the equal of DoD's contribution in other areas such as automation standardization and compiler design. The pace of the research and associated results has, however, been a problem. The state of automation has

moved at a significantly faster rate than has the effort to secure the information being processed, leading to a "security solution gap" that largely remains unresolved. In fact, the gap seems to grow larger each year as advances and capabilities in automation and communication continue to accelerate. This solution gap is worthy of further investigation and in reality it could be viewed as the "risk" associated with the processing of information on a system with a specific set of protections in place. A second observation is that DoD security guidance currently available seems to satisfy problems that existed several years ago but serves limited purpose today in solving problems facing the Office of the Secretary of Defense (OSD) leadership and the warfighting Commander-in-Chief (CINC) community [2]. A third observation is that the community has discovered additional "*types*" of security problems that it has not done a very good job of focusing on and providing solutions to (e.g., continuous availability of systems and data; assurance that the data we access is correct and consistent; or, defining what is "*adequate*" security for unclassified information that is in need of some level of protection). Newspapers and periodicals are replete with examples of instances where security failures occurred because of lack of proper procedure or due to failure to recognize a particular vulnerability. One only has to review, for example, the Morris Worm event [3] [4], the "excessing" of government agency computer equipment with sensitive information still resident on magnetic medium, the mailing of IRS CD-ROMs with a virus present, or the software failure in AT&T's switches only a few years ago in order to recognize the continue relevance of INFOSEC requirements.

1.2 ASSURANCE VERSUS ENVIRONMENT

It can be argued that the assurance required may change dynamically depending on the actual threat environment. Factors such as peace or war, the perishability of information, attacker's capabilities, and importance of the information, all impact the degree of assurance needed. The set of factors relevant to changing security requirements, and therefore reducing or increasing risk acceptance, is directly correlated to the business process associated with the enterprise requiring a security solution. This can be discovered by understanding the enterprise, its processes, threats, management philosophy, and its "reach" (where reach is loosely defined as its connectivity and access). This means that a recipe approach to assurance determination is likely not a good direction and one cannot reduce the INFOSEC problem to that of a "commodity selection," which seems to often be an accepted approach. Section 3 of this paper will describe some thoughts for a change in this approach—one of which is consistent and adaptable to the process described in Section 2. If one accepts the premise that there is no such state as "absolute" security, then the INFOSEC problem is reduced to one of *assurance-based-risk mitigation*. As circumstances change, a senior manager must have the ability to take more or less risk based on judgment, understanding and knowledge. Current processes normally don't account for this capability, and as a result, guidelines are often issued that restrict the user to a set of requirements that are inflexible regardless of the changing environment. It is suggested therefore, that there may be value in looking at a user's security needs and solutions with respect to a set of environmental conditions and factors so that more flexibility can be accorded as the environment changes. This is not unlike the Defense Condition (DEFCON) procedures used by the DoD to increase readiness posture of units as the threat conditions change. Consider, for example, a case where a database contains attack plans and other highly classified information that must be shared

among geographically dispersed units, yet remain protected from hostile intrusion. The protection afforded this information might need to be stronger in peacetime when it is being stored, and when the attacker has time and energy to devote to penetrating the system. If the attack plans are placed into motion, the security environment changes and perhaps the protections afforded the information can be relaxed based on the increased perishability of the confidential information, and the reduced time the attacker has to retrieve the secrets. Security models and procedures today do not exhibit this degree of flexibility and DoD senior managers are sometimes placed in a position of making INFOSEC decisions in a vacuum or feeling constrained in accomplishing their mission.

1.3 A SUFFICIENCY APPROACH

Sufficiency in INFOSEC [5] is achieved when the solution's cost, in operational terms, does not exceed its value in terms of the protection it affords. The approach described here to provide a customer with "sufficient" information security services offers a possible framework and a defined process that can be applied throughout the DoD as well as other federal or commercial enterprises. In general, this process is continuous, cyclic, and involves first, a business enterprise analysis (consultancy and/or process definition) followed by security definition, a full-risk analysis, vulnerability analysis, an engineered solution (with alternatives), testing, implementation, education, documentation, and continuous review. These component activities are briefly described in this paper. Following the process description, an argument for change in the DoD approach is presented.

2. THE PROCESS USED

The process advocated in this paper is graphically depicted in Figure 1. It is a flexible process that is designed to accomplish a full understanding of the customer's need, the engineering of a solution based on need, the development of processes that support the solution internally, and continuous review and improvement.

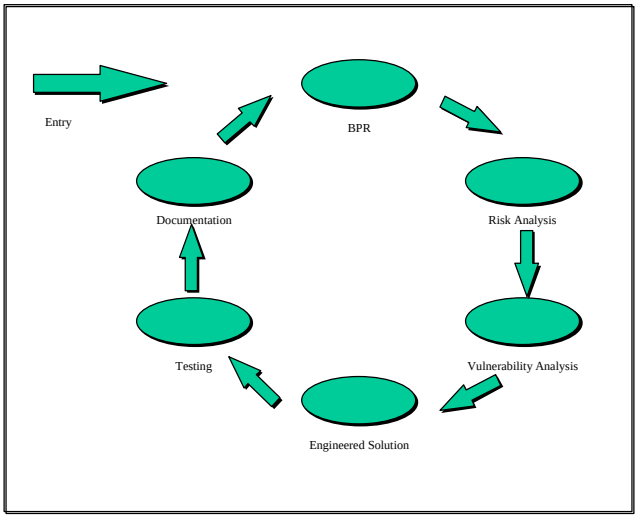


Figure 1: Cyclic Process to Determine Sufficiency (assumes continuous review).

2.1 PROCESS COMPONENTS

A high-level description of each component of the process depicted in Figure 1 is provided below. It is of key importance to note that the process is cyclic and repeatable. Providing a secure environment for a customer can only be accomplished if one periodically reviews the state of technology, the threat, the environment, the customer expectation, etc., to insure that the solution installed yesterday is still meeting requirements today. Furthermore, testing and documentation are considered an integral part of the process - testing builds confidence on the part of the customer and documentation (to include training), provides guidance to those that must use the system and alerts them to the threat and the rationale for the procedures put in place.

a. Business Process Review (BPR): The first step in securing enterprise data should be an in-depth look at the enterprise itself: the information flows, the determination of what needs to be protected, a clear understanding of what is meant by security, and perhaps the building of an "as is" model and a "to be" model that embraces data protection as one of its principles. This is the requirements gathering phase which influences all activities that follow. Security is a mission critical function that must be incorporated into the business enterprise of an organization as a whole. It not only impacts the enterprise, but often affects customers and other enterprises as well-depending upon the enterprise reach and its processes. Today's social, cultural, technological, economic, political and legal macro-forces require that organizations understand the implications of these influences. The BPR is structured to accommodate these forces and to determine how the enterprise views security and what is expected of a secure solution. In the process of conducting a BPR, a security model is developed that defines the security rules and procedures that must be enforced. Additionally, this model becomes a shared mechanism between the INFOSEC analyst and the customer to achieve a common understanding of the end objective. It is during the BPR that a clear understanding of the problem is achieved, and a plan of action is developed that leads to a desired end state (or "to be" model). Additionally, the BPR begins to establish the definition of enterprise reach—or, who else is affected by the solution that is (or is not) imposed on the system. Reach determination is important in that a decision maker must understand the full impact of any decision that is made with respect to the security of the system. In some cases, other decision makers must be consulted or informed of enterprise actions. Reach is also a key factor in assisting management and analysts in defining the "security perimeter"—or bounds of protection. Normally, senior management from the customer's organization is heavily involved in this process. An important by product of this BPR is a determination of the various environments in which the information requiring protection will exist. It is possible that different protection requirements will be associated with different environments. Other factors such as perishability of the data, risk of loss, value of the data, etc., are discovered and recorded.

The notion of a "System Security Environment" can be defined as follows.

DEFINITION: SYSTEM SECURITY ENVIRONMENT. A system security environment, *v*, is an element of the set of possible security environments V that may be defined as three tuple:

V = [S, A, F], where

S: is the set of possible system states of existence, s_i, in which a defined risk has been identified and a set of protections have been put in place to mitigate the risk.

A: is the set of actions, a_i, that move the system from one state to another.

F: is the set of key protection factors, f_i, associated with a specific state, s_i.

It then becomes the job of the BPR analyst to work with the enterprise to discover those pairs, (s_i, {f_j, ~~V~~$_j$, j= 1, n}) which represents a specific plausible environment and the specific factors of protection that are important to the enterprise. The set of actions are essential to the analyst's task to ensure proper INFOSEC coverage. The BPR phase does not enter into problem resolution - its objectives are problem determination, desired end-state security, and the establishment of a common understanding between the customer and the engineering team.

b. Risk Analysis: A risk analysis is a high-level review of what we are protecting against. It focuses on determining the most likely and least likely threats. The risk analysis should be repeated for all plausible environments – e.g., peace, war, crisis, insider attack, external attack, etc. The environments should have been determined during the BPR, and each should have risk associated with them. The objective is not to find a solution for each environment, but rather to understand what protections are needed and when. A most difficult part of this step is to determine what is the "security perimeter" that we are responsible for protecting. The security perimeter is the boundary within which we guaranteed an agreed upon level of protection, and outside of which we offer no guarantees. Understanding the enterprise and its reach is essential to this task.

c. Vulnerability Analysis: Once the risks are determined, it is important to define what is actually at risk – this constitutes the vulnerable components within the security perimeter and assists in identifying what protection mechanisms are needed (products, assurances, procedures, civil works, etc.). Often, a risk analysis and vulnerability analysis are considered one and the same. There is, however, a slight difference. While the risk analysis focuses on what the threat is and where it is likely to come from, the vulnerability analysis determines what it is that the threat is likely to attack (and how successful the attack is likely to be). The BPR results are needed here to gain a clear understanding of what the customer will consider a security breach—

issues of confidentiality, availability, accountability, consistency, and integrity may be discussed and evaluated in light of the customer's view.

d. Engineered Solution: We define sufficient levels of protection during the engineering solution phase. INFOSEC analysts are employed to recommend adequate protections to mitigate the identified risk in specific various environments and, more importantly, to identify those areas of risk (or weak assurance) that remain once a technical solution is offered. Additional modifications to the enterprise's procedures, physical environment, documentation, awareness, or personnel policies are then offered to further mitigate the remaining risk. It is here that "assurance" plays an important role. Since assurance relates to the strength of the mechanisms employed by the engineers, it is of extreme importance that the engineer have a full understanding of the customer's expectation and need (from the BPR), as well as the strength of the mechanisms being recommended and integrated into the solution set. There is never the luxury of a 100 percent solution. The protection environment offered to the customer must be robust enough to offer a reasonable solution that provides sufficient strength such that compromise or penetration is not likely or such that the risk of such activity is acceptable. This implies that the customer must also be told what risk has not been mitigated by technology and advised in how to best minimize the residual risk through procedures or other means. When the total solution is presented, there will be risk, but it will be identified, accepted, and known. There will also be a range of solutions presented that must be coupled to a particular "state of the enterprise". Through this process, management will be given alternatives that equate to operational conditions and will, therefore, be of assistance in the decision process that must occur when the state changes.

e. Testing: The solution is tested with an agreed upon set of test procedures that represent reasonable risk expectations and, if successful, offer a high degree of confidence that the protections employed actually meet expectations. This phase is still more of an art form than a perfect science. Testing comes in many forms. It can include a formal proof of a model, a mapping between model and specification (or specification and code), penetration testing by specialized teams, standard test cases developed against a set of specifications, or open and continuous testing from the attacker community itself. (Note: This last method has been successfully employed by Secure Computer Corporation in testing its Sidewinder firewall product against Internet penetration). If at all possible, testing should be accomplished by a joint team of customer (functional and technical) and contractor personnel.

f. Documentation: Specific, detailed documents are provided to the enterprise that outline the procedures, practices, and engineering changes. Additionally, an "awareness" training program is often instituted. The degree to which the documentation and training tasks are accomplished is largely dependent on the customer, the risk identified, and the current state of awareness that exists within the

business enterprise. If the customer is a Government activity, there are likely specific deliverables called for by security policy. These might include: a Security Features User's Guide, a Trusted Facilities Manual, a Certification Study, a Security Operations Manual, and/or others. For a commercial customer, documentation is likely to primarily consist of operations manuals and an overall procedures guide. In all environments, the sufficiency approach should result in an additional document that one does not normally consider today—this is an operational procedure that modifies (in a controlled manner) the security perimeter based on clearly defined business states and decision authority. Training is considered essential in all customer environments—without a full understanding of the threat, the risk, the mitigation strategy, and the vulnerability on the part of the workforce, the security perimeter will be weakened by the insider workforce (unintentionally or intentionally) through a lack of understanding. Provision must be made for periodic training to accommodate the need for reinforcement in the workplace and to train new members of the workforce. Naturally, the extent of this training and its frequency is determined in conjunction with the customer and the perceived need.

g. Continuous Review: A periodic review of the risk, vulnerability, system changes, management changes, technology changes, etc., is required to insure the adequacy of the solution. Failure to do so may result in insufficient protection as mechanisms become aged and attackers become more proficient. The timing for such reviews is very enterprise dependent.

2.2 PROCESS SUMMARY

This approach is applicable for all definitions and views of security – e.g. confidentiality, accountability, integrity, and/or availability. The approach is flexible, involves the customer, is documented, and is constantly improved upon. It identifies risk that is mitigated by technology, practices, and procedures, as well as identifying the risk that remains. Most importantly, it establishes a customer definition of security early in the process, develops a customer expectation of what is to be achieved (the desired end state), and identifies what security risks have not been mitigated. It provides management authority a tool from which operational decisions that affect enterprise security can be made in a controlled and knowledgeable manner. The process is applicable for the US Government, international, and commercial enterprises. It is not dependent on a particular set of regulations or directives and is adaptable to the customer's environment. It is solution oriented but does not overly restrict in the sense that it incorporates flexibility by advocating a range of protections dependent upon the environment.

3. THOUGHTS FOR CHANGE

3.1 THE CURRENT APPROACH

Within the DoD there is an abundance of regulations and guidelines that are designed to provide for security of information processing systems with great assurance that risk of data compromise is minimized to an acceptable level. Unfortunately, the area of risk reduction is not well understood except by those who work in this highly specialized area. Those that have the *responsibility* and *obligation* to protect data assets are generally at the management level, have little background or training in information security, and feel constrained by rules they neither fully comprehend nor appreciate. In an effort to make the whole issue of INFOSEC easier to apply in this setting, it appears that DoD often tries to oversimplify security technical aspects for the ease of management application. An example of this might be the DoD 5200.28-std (Orange Book) publication where INFOSEC assurance was reduced to a hierarchy of digraphs organized from a low of C1 to a high of A1. A set of rules were then developed around these digraphs to make system selection "easier" for those communities that had a need to process classified data. Multilevel security was essentially assigned to only systems having a B1/B2 or above rating while some dedicated and system high modes of operation could be run on systems having a C2 or above rating. Catchy phrases like "C2 by 92" were coined and found their way into regulatory guidance. Industry was expected to comply with this philosophy and develop such high assurance systems with a promise that "if you build them, we'll buy them". This approach was never successful - for many reasons, not all of which are reported here. It was over constraining, the technology of networking overtook standalone processing, vulnerabilities not well understood initially were later discovered, viruses and worms (and other forms of malicious code) were introduced, the Internet explosion created a whole new problem set to address, electronic commerce rose to the forefront, and other advances too numerous to detail here have occurred. The initial approach to securing systems was not wrong - just constrictive and promised too much. It was, however, based on solid and fundamental technical principles that still are essential and apply today. Additionally, it was never well understood by those who had the responsibility to accredit the systems. Today, the defense community still has trouble connecting its disparate email systems together that have varying degrees of security classifications; air gaps or sneaker nets still exist between warfighting systems; high assurance operating systems have never been built in the numbers envisioned nor have those that were built sold to any great extent; and, still the overall security regulatory environment remains rather inflexible regardless of dynamic changes which occur outside security perimeters. An ancillary concern is that early rated systems may not today possess the strength they were originally thought to have – further evidence that we do not deal well with the dynamic nature of the security problem.

3.2 AN ALTERNATIVE VIEW

As a thought, perhaps security of systems could be viewed in three distinct tiers of concern (regardless of the security problem being solved). Tier I might represent the "high end" of security in the federal government and is characterized primarily by the intelligence community and the data it owns or originates. Tier II represents the DoD/federal government non-

intelligence security problem. Tier III is primarily the commercial market place. Each tier has different requirements and, in some cases, different views on what security really is. Most certainly, each tier has a different need for assurance in its INFOSEC solution.

a. Tier I. The Intelligence world demands security to protect the confidentiality (primarily) of its high valued information. This information is most often classified as Top Secret and may include some special category restrictions. The customer for these systems must have high assurance systems and would like to have reliable multilevel secure systems on which to access the data. Unfortunately there are few, if any, of the products that both meet the government's specifications for such Multilevel Secure (MLS) capability and have the full confidence of the intelligence community. The result has been a continuing reliance on dedicated and system high processing with air gaps between this community and its Tier II counterparts. It is the opinion of this author that not much is likely to change in the foreseeable future and this community will continue to distrust MLS technology and will not accept any risk of compromise short of "absolute security". One could also submit that the Tier I community is not likely to see any environmental changes that would cause them to relax these inflexible rules - the risk of compromise is just too great.

b. Tier II. The non-intelligence DoD/federal government customer has a different problem and can afford to look at a range of protections based on its environment. This tier does have some Top Secret data to protect, but the vast majority of its confidentiality problem is at the Secret, Confidential, and Sensitive but Unclassified (SBU) level. In fact, empirical data would suggest that the majority of protection requirements are at the SBU level. The integrity and availability concerns also seem to be more pronounced at this tier than at Tier I. Flexibility is possible at this tier and the process described in paragraph 2 above can be used to determine the full range of flexibility needed based on the specific customer and the technical products available to mitigate risk identified. It is here that management is often willing to assume risk - especially if the risk can be identified and if the attacker is not likely to resort to the efforts necessary to penetrate the system. A recent example of just this scenario occurred with the deployment of our forces to Bosnia. A major computer services company was contacted by a DoD customer to assist in bypassing certain security mechanisms that were put in place as a firewall during peacetime to protect a logistical database from Internet attack. When the US forces deployed and were forced to use the Internet for access to this SBU data, the contractor responsible for maintaining the database refused to bypass the firewall for fear of violating government regulations and exposing the database to integrity problems. The customer - frustrated and willing to accept limited risk - came to another commercial enterprise requesting the installation of a dedicated T1 line into the database that bypassed the firewall so that forces in Europe could conduct their mission. In this case - a change in the environment brought about a change in acceptable risk. This is an excellent example of trade off of acceptable risk for the sake of operational cost. The problem occurred in trying to exercise any options for increasing risk. There should have been an expectation that under certain circumstances, different security procedures would be

adopted. This same scenario can be played out a number of times in the Pentagon and throughout the services.

c. Tier III. This represents the commercial market place where the customer is far more flexible, yet has the same degree of security concerns found in the tiers above. Often, however, their concern is in protecting data from unauthorized modification and unauthorized viewing, as well as insuring that the data remains available and actions are accountable. The process described in this paper is directly applicable and likely acceptable to this community also.

4. SUMMARY AND CONCLUSIONS

A process has been described herein that approaches security solutions by understanding the enterprise, determining where it wants to go, engineering a solution based not only on the present operating environment, but also on other potential environments that might result in a change in assurance provided or required by the customer. The premise suggested is that one wants to establish "sufficient security controls" for the protection of the data, yet remain flexible enough to modify that environment as the need arises. Risk analysis and vulnerability analysis were described as an important part of the process in order to understand what the threat was and what is at risk. The process includes the customer and insures that customer exceptions and needs are met through a continuous understanding developed throughout business process modeling and dialogue. It is suggested that a range of security controls is appropriate in most cases and that this philosophy should be considered for adoption by DoD in most circumstances as a way to increase the data owner's flexibility in protecting information assets in various environments. The process discounts a "cookbook" approach to security as too rigid and overly conservative. Instead, defining the risk to the risk taker is promoted as a better approach in most cases (excluding Tier I).

5. ACKNOWLEDGMENTS

I wish to acknowledge several individuals who encouraged me to submit this paper to this conference. First, my good friend Dr. Ron Ross of NIST who has constantly responded to my many emails asking for advise and assistance throughout the many years we have been friends. Second, Dr. Marshall Abrams, who constantly encourages me in this academic field of study. Lastly, Dr. Julia Hodges, the Department Head of Computer Science at Mississippi State University who has allowed me to pursue this subject as a field of academic endeavor and has encouraged me to seek associated research funding to build a security program at MSU.

6. REFERENCES

[1] DOD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, Dec 1985.

[2] Feustel, E & Mayfield, T. "The DGSA: Unmet Information Security Challenges for Operating Systems Designers.", Operating Systems Review, vol 32, no 1, Association for Computing Machinery, New York, New York, pp. 3-22, Jan 1998.

[3] Eichen, M. & Rochlis, J. "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988.", Proceedings IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 1989, pp 326-343.

[4] Spafford, E., "The Internet Worm: Crisis and Aftermath." Communications of the ACM, vol 32, no. 6, June 1989, pp. 678-688.

[5] Vaughn, R., "A Practical Approach to Sufficient INFOSEC.", 1996 DOD Software Technology Conference, Salt Lake City, UT.

21st National Information Systems Security Conference

A Practical Approach to Sufficient INFOSEC

Some Cautions

- These Opinions are My Own
- The Process Described is Very High Level
- The Purpose is to:
  - Promote Change and Flexibility
  - Become More Realistic
  - Evoke Discussion

Why?

Because We:

- ☺ Have A Good Theoretical Foundation
- ☺ Have Products
- ☺ Understand the Problem
- ☺ Continue to Make Progress

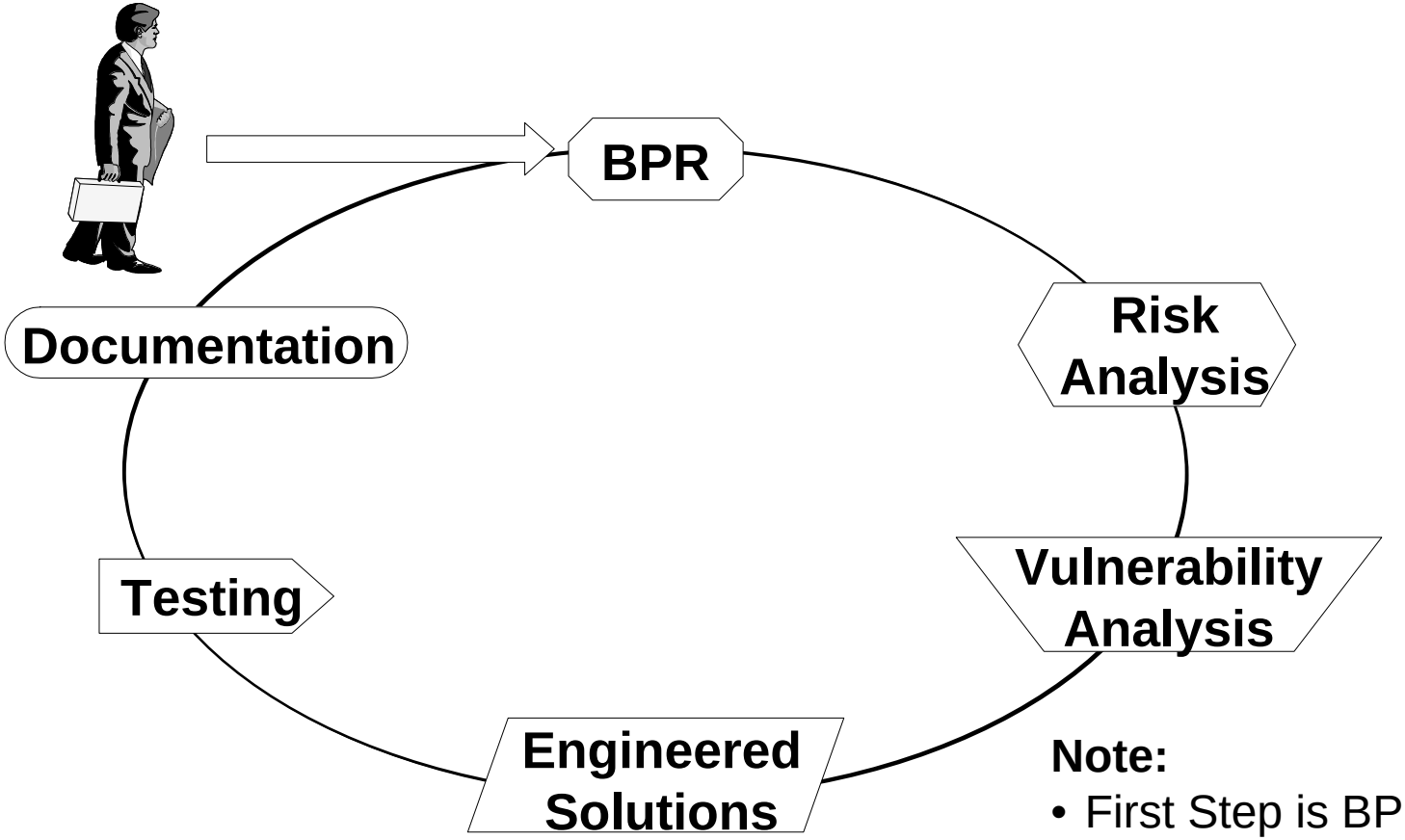
. . . But!

- ☹ Products Do Not Match Problems
- ☹ Rigid Controls Have Operational Impact
- ☹ No Flexibility
- ☹ Solution Gap Continues to Grow
- ☹ Rapidly Evolving Technology

So, Let's Think Outside The Box!

- Is All Security the Same?
- Does the Problem Change Dynamically?
- Are Security Attributes of Data Static?
- Should Operational Commanders Have More INFOSEC Flexibility?
- What is "Sufficient" Security?

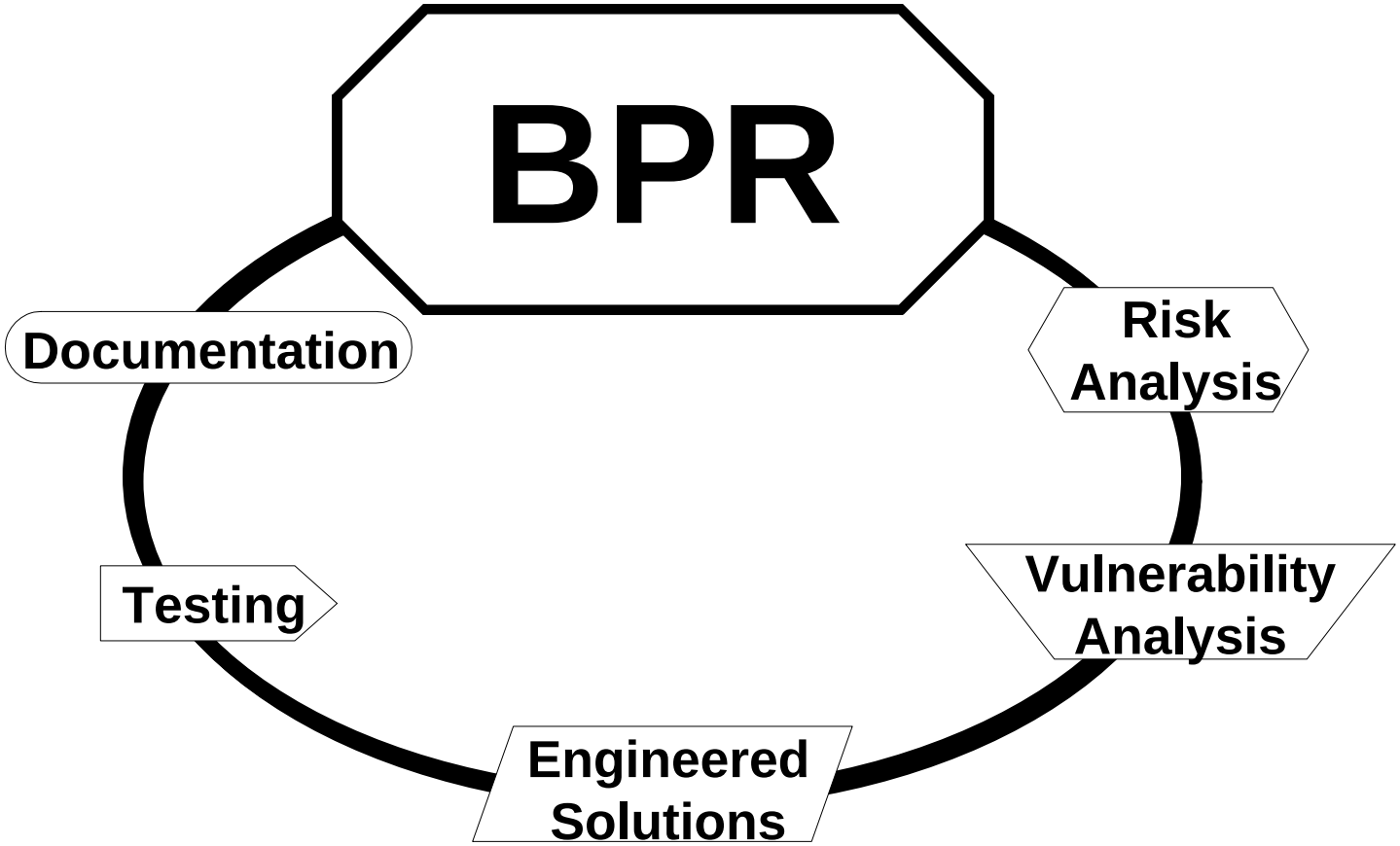
A Process



Note:

- First Step is BPR
- Cyclic
- Regulates Participation of Enterprise

The Process


BPR
Risk Analysis
Vulnerability Analysis
Engineered Solutions
Testing
Documentation

BPR Is Key!

- “As is” vs. “To Be”
- Security Model
- Involvement of Management and Analyst
- Knowledge of:
  - Reach
  - States
  - Protection Factors
  - Cause and Effect

Reach

Answers the Questions:

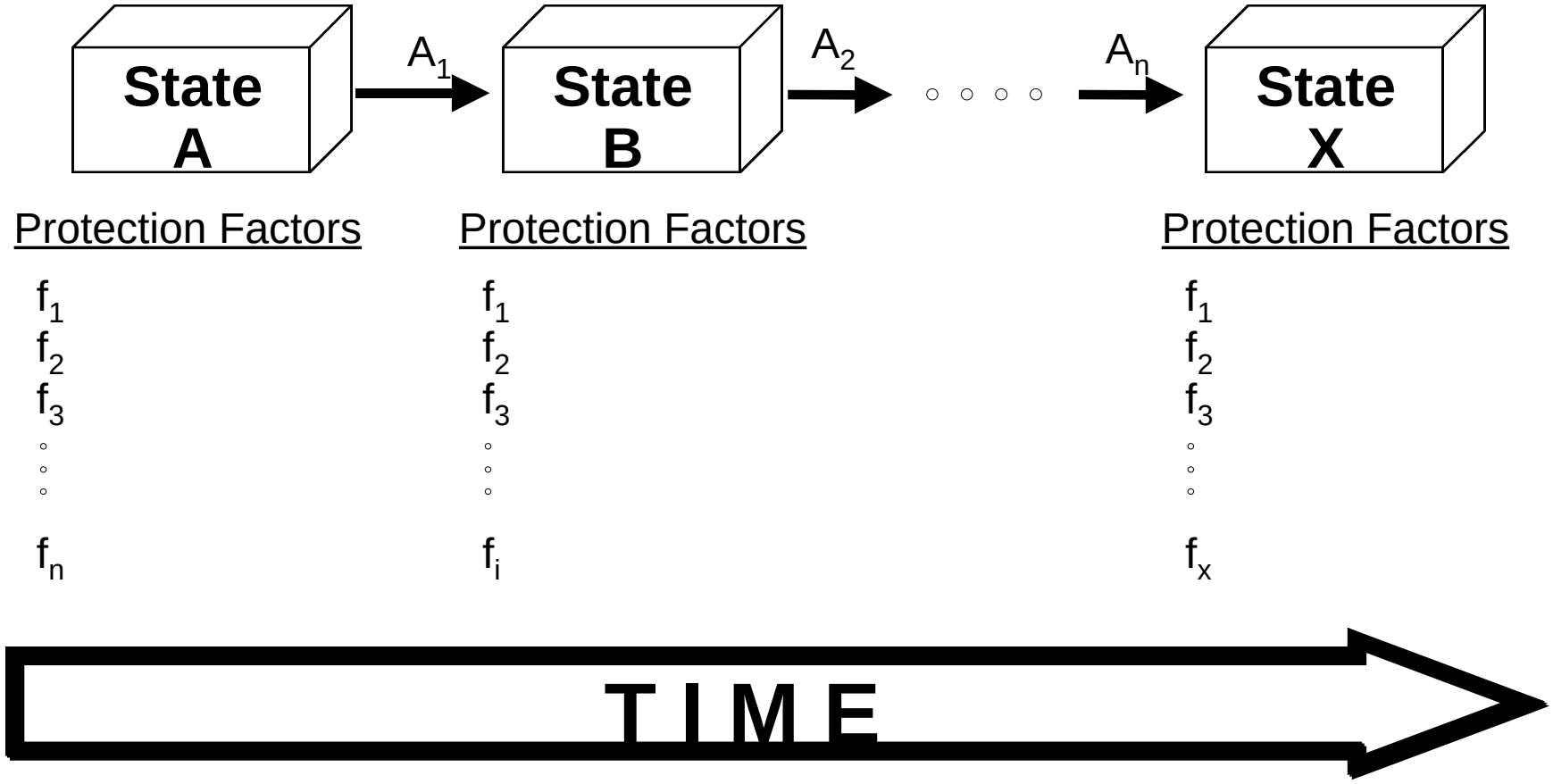
- Who Else is Affected?
- Who Else Cares?
- Customer Impact?
- What is the Net Effect of a Change to the Security Perimeter?

System Security Environment

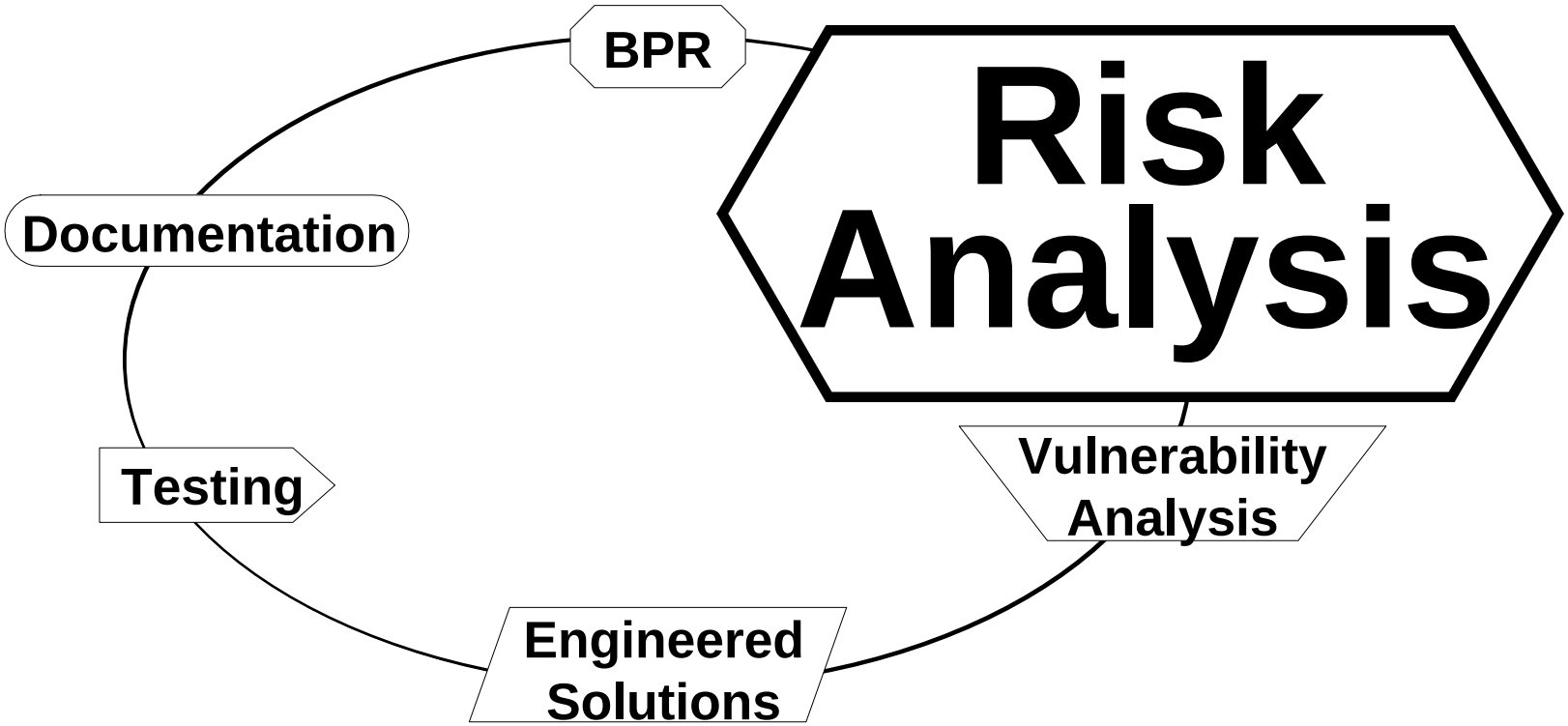
Consists of Three Important Elements:

- A Set of Enterprise States in Which There is a Defined (or Identified) Set of Risks
- A Set of Actions that Move the Enterprise From One State to Another
- A Set of Key Protection Factors that are Associated with a Specific State

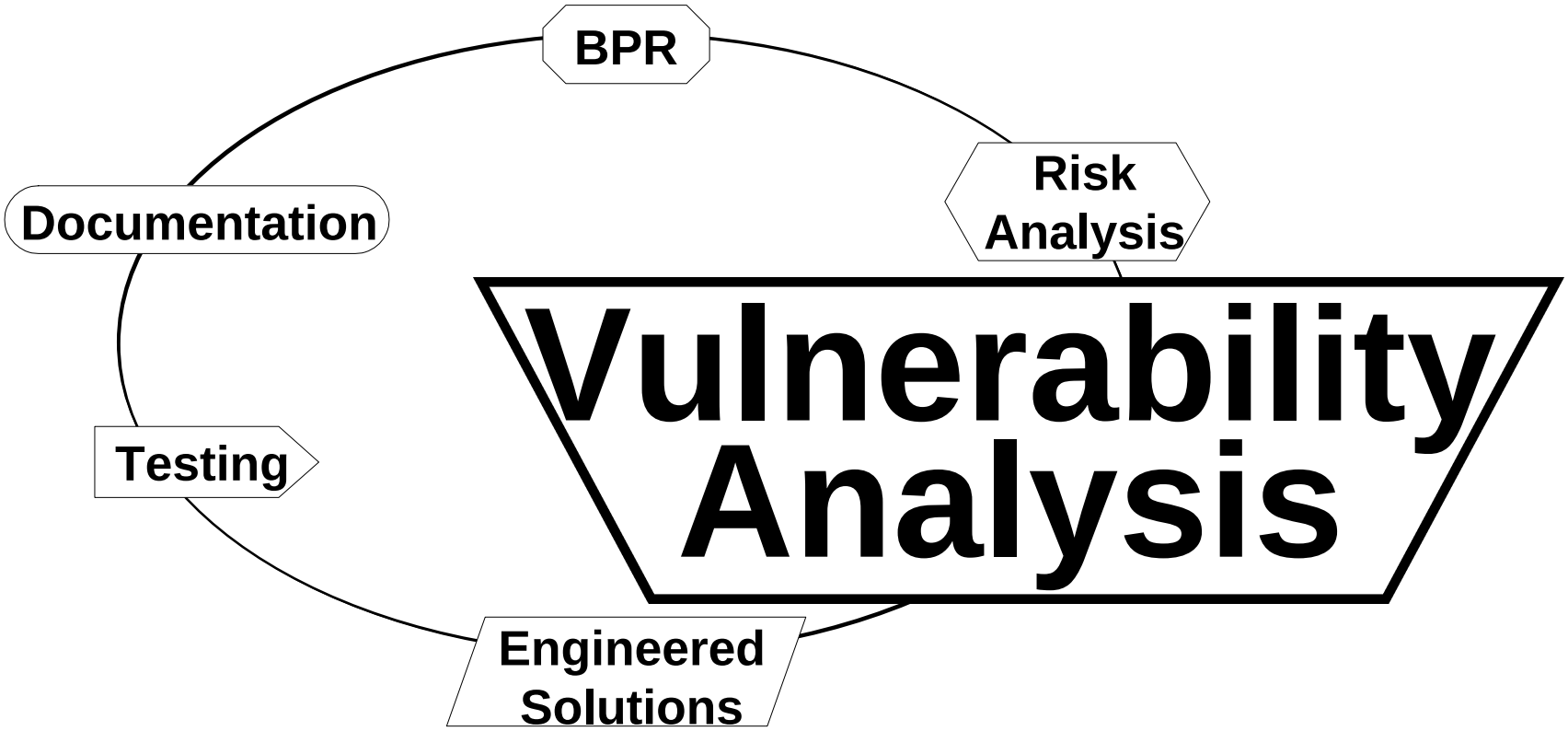
The State Of An Enterprise Is Not Static!



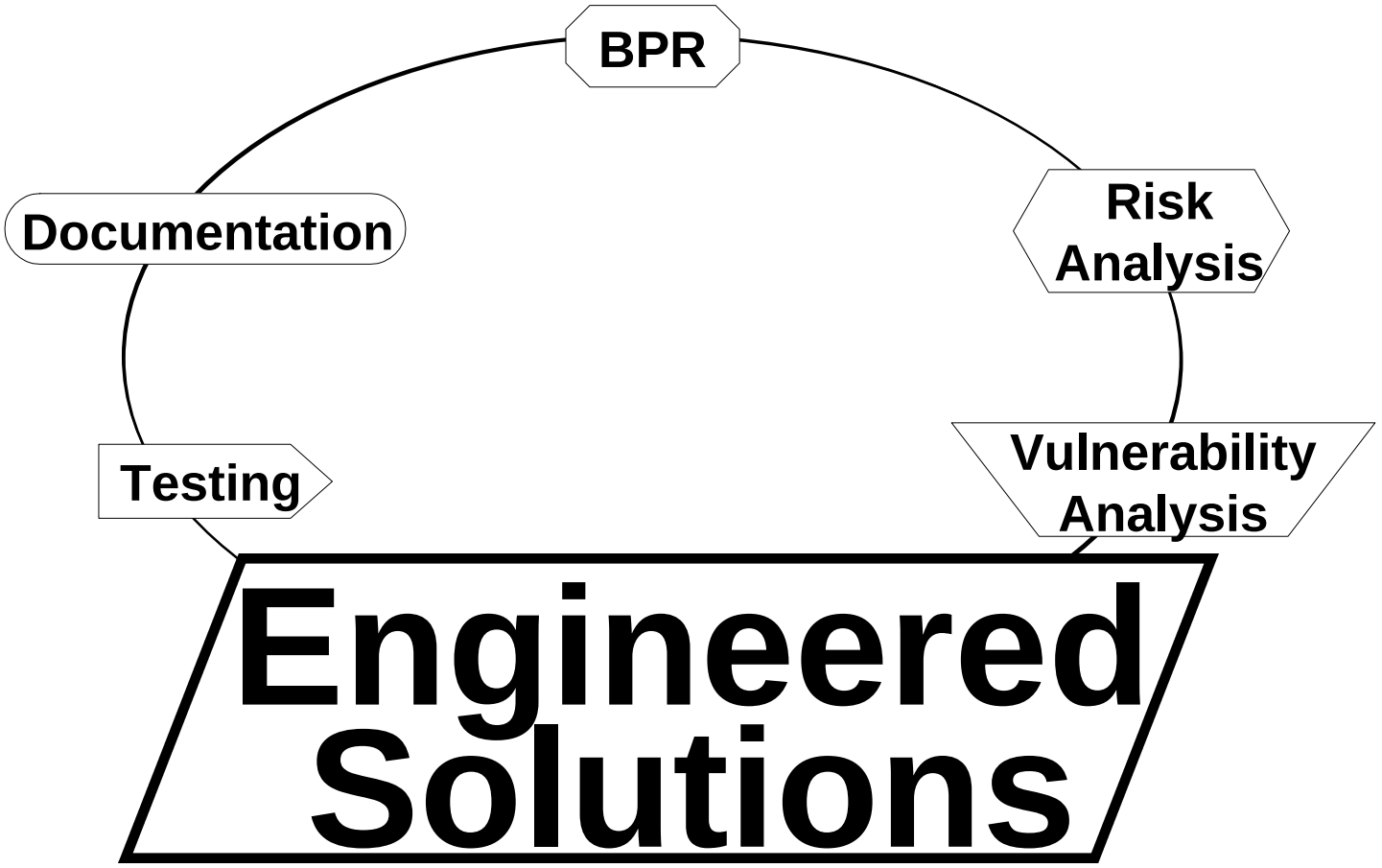
The Process


BPR
Risk Analysis
Vulnerability Analysis
Engineered Solutions
Testing
Documentation

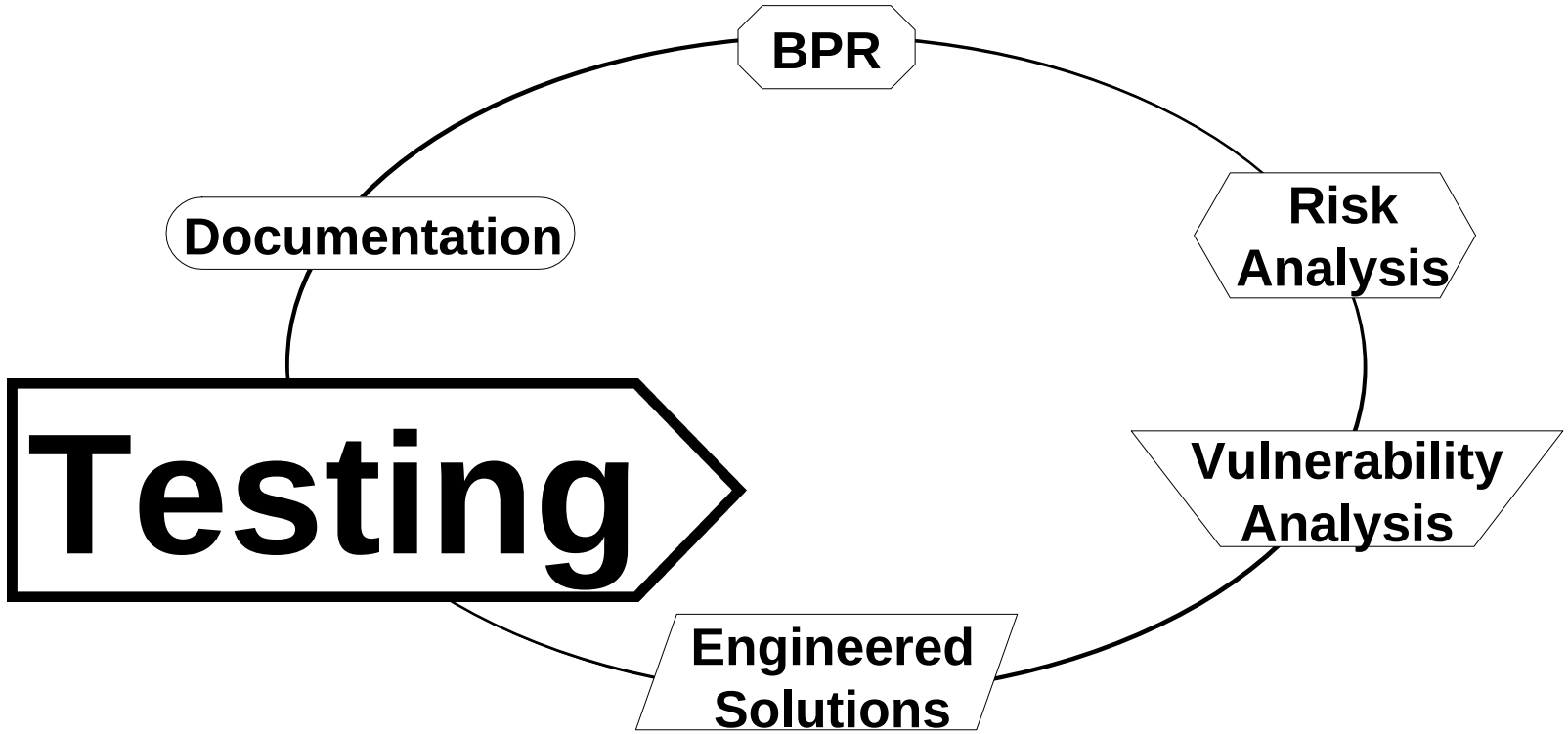
The Process


BPR
Risk Analysis
Vulnerability Analysis
Engineered Solutions
Testing
Documentation

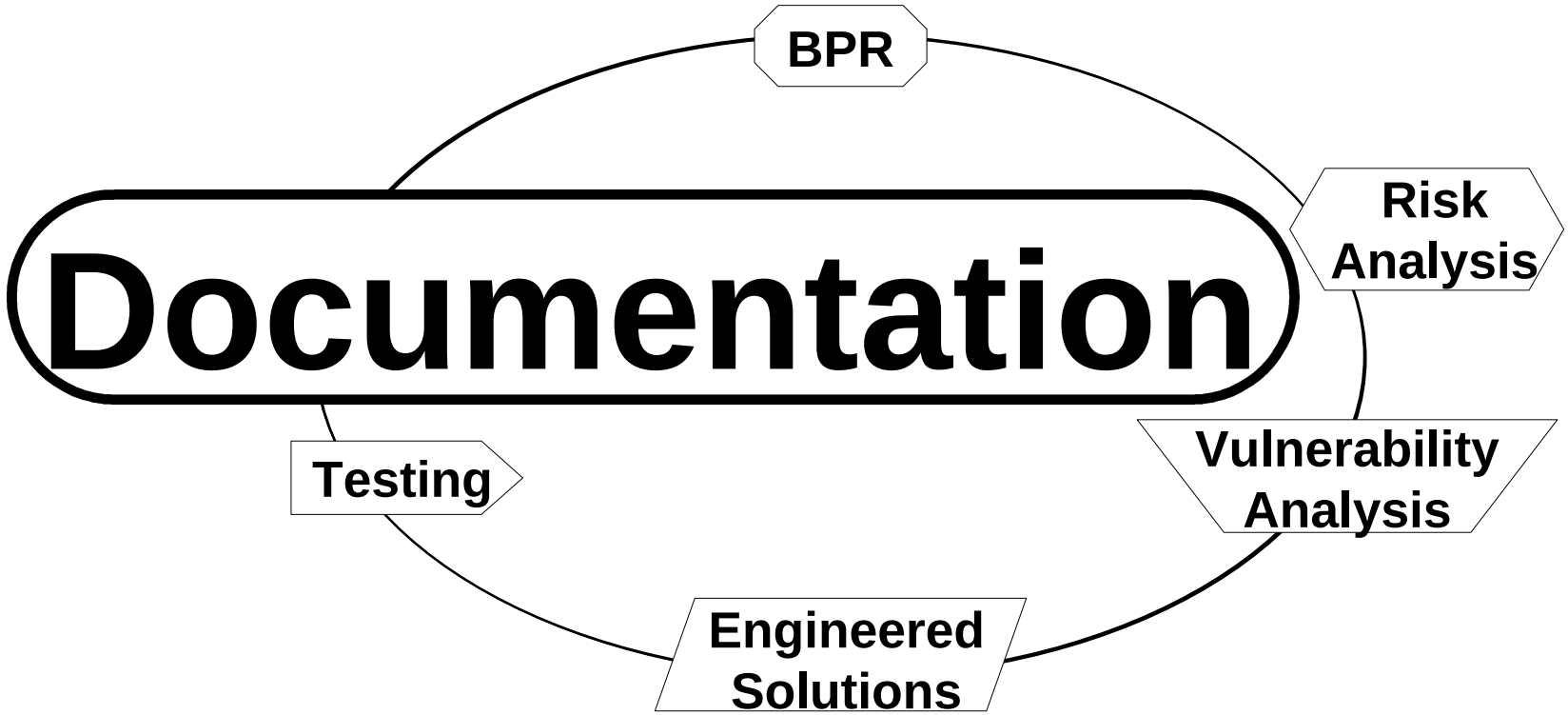
The Process


BPR
Risk Analysis
Vulnerability Analysis
Testing
Documentation
Engineered Solutions

The Process


BPR
Risk Analysis
Vulnerability Analysis
Engineered Solutions
Testing
Documentation

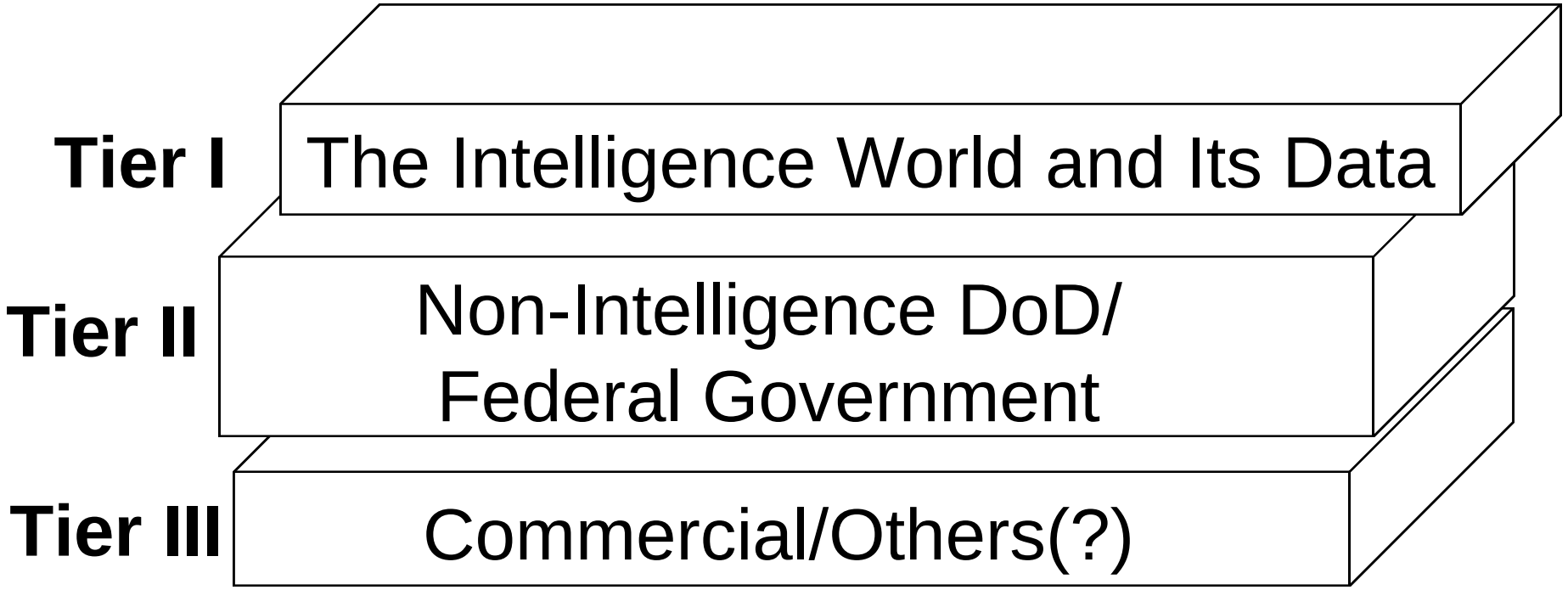
The Process

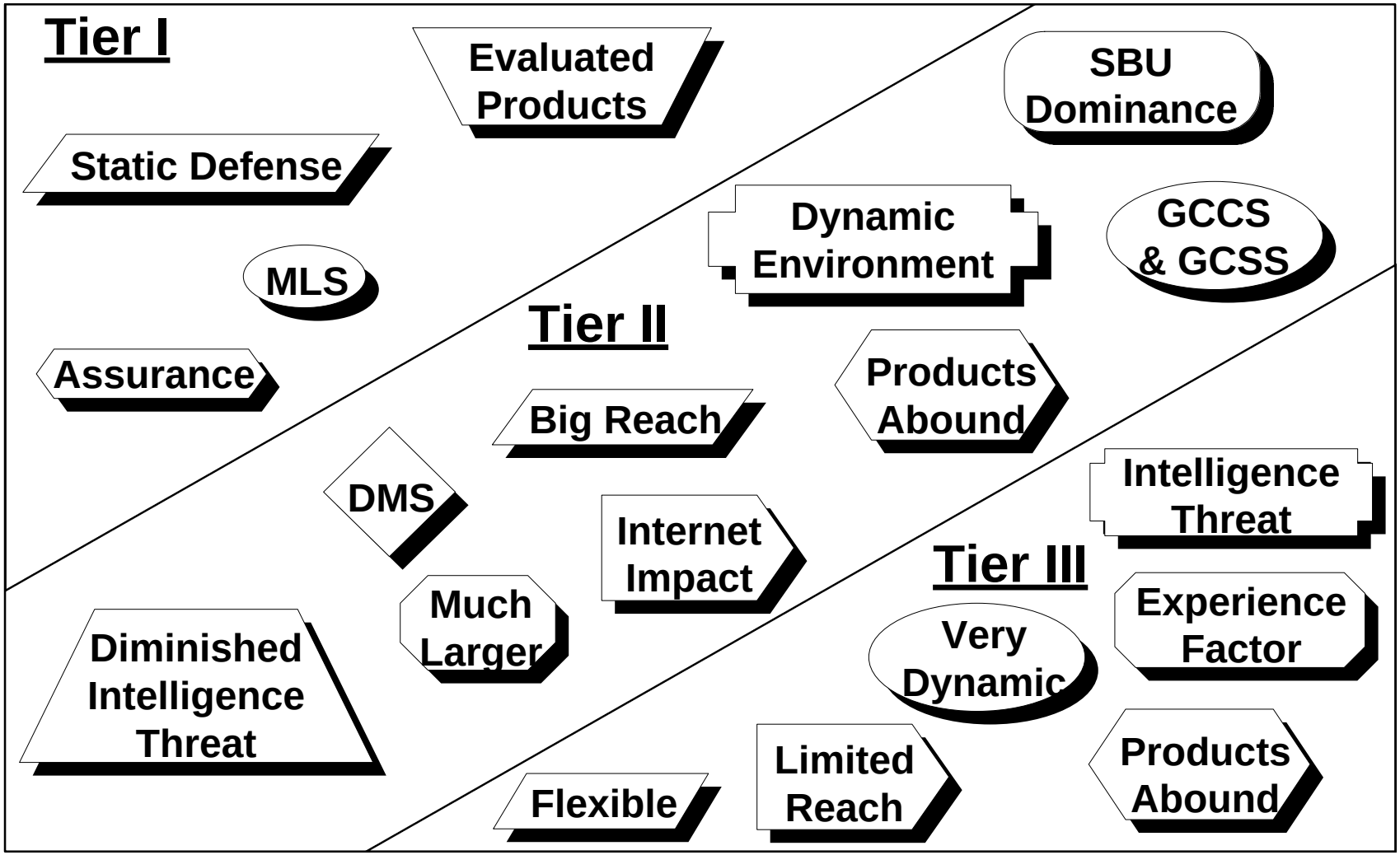

BPR
Risk Analysis
Documentation
Vulnerability Analysis
Testing
Engineered Solutions

Thoughts For Change

- DoD Has Historically Viewed INFOSEC as a Static Defense - Not Dynamic
- Difficult to Apply Current Regulatory Guidance Across the Whole Spectrum of INFOSEC
- “Work Arounds” Abound!
- The INFOSEC Promise is Still at the End of the Rainbow!

Three Tiers - Three Problems




Tier I
Evaluated Products
SBU Dominance
Static Defense
Dynamic Environment
GCCS & GCSS
MLS
Tier II
Assurance
Products Abound
Big Reach
DMS
Intelligence Threat
Internet Impact
Tier III
Much Larger
Experience Factor
Diminished Intelligence Threat
Very Dynamic
Limited Reach
Products Abound
Flexible

Maybe We Should . . .

- Leave Current Restrictions in Place for Tier I
- Modify Approach for Tier II and Adopt a Process That Allows Flexibility
- Give Commanders Authority to Execute Contingency INFOSEC Modifications
- Rely More Heavily on Industry's Product Base

Wrap Up Thoughts

- Risk is That Area Where Protection Ends and Threat Begins
  - *It Cannot Be Reduced to Zero*
- Risk Changes Based on A Set of Actions
- Managers Must Be in a Position to Respond to Change - With Plans
- The Process Briefly Discussed Here Can Be Useful in Tier II and Tier III Solutions


Questions?