ASSESSING THE POLICY DIMENSION

T Grobler, Prof SH von Solms

Technikon Witwatersrand

RAU Standard Bank Academy of Information Technology RAU University, Johannesburg, South Africa

talania@twr.ac.za, basie@rkw.rau.ac.za

011 406 3552 / 489 2847

ABSTRACT

Information is the most important asset that must be secured in any organization. The integrity, availability and confidentiality of information will enable an organization to maintain competitive advantage in the marketplace.

Information Security is a multi-dimensional discipline. The following dimensions of Information Security can be considered to obtain a holistic overview of the security of an organization: Corporate Governance (strategic and operational), Policies, Risk management, Legal, People, Compliance and Technology. The dimensions do not exist in isolation, but are interrelated.

This paper will discuss the importance of the Policy Dimension and discuss the relation of the Policy Dimension to the other dimensions. It will also discuss elements of the Policy Dimension and propose that an organization should set up a policy framework.

The paper will propose an assessment model to use when assessing the Policy Dimension. Assessment of the Policy Dimension will not concentrate on compliance to policies but rather on determining whether the policies defined for the organization are comprehensive, up to date, complete and delivered in an effective way to your employees.

The paper will not provide a detailed assessment plan, but a high-level overview of the assessment model. Management will be able to obtain a visual overview of the current status of the Policy Dimension.

KEY WORDS

Information security dimensions, Policy, Assessment model, Policy framework

1 INTRODUCTION

Information Security can be defined as the process of protecting information systems and hardware that use, store and transmit the information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize the return on investment by preserving confidentiality, integrity and availability of information and information assets.

Every manager should be able to determine how well Information Security has been implemented in the company and how it compares to other companies in the same industry. It is important to assess the effectiveness and efficiency of the security (people, processes and technology) implemented in your organization to justify the money invested in security.

Information Security is a multi-dimensional discipline. Some of the dimensions identified by Von Solms are Corporate Governance (Strategic and Operational), Policies, People, Best Practice, Legal, Certification, Insurance and Audit. (Von Solms, 2001a]. The list may not necessarily be complete, because there are no fixed boundaries to the dimensions.

Quality security programs begin and end with policies. Well-defined policies will enable managers to manage the employees in the organization efficiently and effectively. Policies are the least expensive control to implement, but the most difficult to properly manage.

Organizations must manage security in a structured, holistic way. An Information Security Architecture will provide management with a blueprint to manage. The architecture must be supported by guidelines to specify what should be done and how it should be done. These guidelines must be documented in the form of policies, standards and procedures. It is important that the policies support the overall strategic objectives of the organization.

A single policy will not be able to provide a solid foundation for the development and implementation of secure practices in an organization. Organizations must develop various supporting policies to address specific issues such as access controls, permissions or physical security. A well-structured organized policy framework is needed to enable management to manage all the risks associated with security.

Even state of the art technologies can be undermined – or rendered ineffective – by poor policies or operational practices. The human element is often the weakest part of the process and should be scrutinized when designing policies and procedures.

2 DO POLICIES GUARANTEE SECURITY?

Companies invest large amounts of time and money in developing comprehensive security policies. There is a perception in industry that a clear correlation exists between security policies and effectiveness of security implementation in an organization. The big question remains: *will the organization be more secure*?

A security survey by CII-PwC in 2002 illustrated that, although most companies had comprehensive formal policies in place, the effectiveness of the security was still relatively low, as 60% of the respondents were hesitant about the security effectiveness and 17% were still completely insecure (Mohan, 2003)

The reasons from the survey for this contradiction were

- Organizations do not perform proper risk analysis before developing policies
- Lack of understanding of policies
- Security policies are not used to manage risks
- No awareness programs or user training programs are in place

- Policies are not reviewed regularly
- IT departments develop policies bottom-up not aligning them to business objectives
- Policies are not managed and implemented
- Organizations must determine if the policy is being followed

It is important to develop and maintain healthy security policies. There are additional natural weaknesses to consider when developing and assessing policies.

- **Security is a barrier to progress**. Security measures, even friendly and easy to implement, will reduce productivity. The measures will mitigate the threats but typically do not add additional benefits to business processes and sharing of information. It is essential to determine the impact of the security on the business processes and the users. Users can ignore policies due to the impact of the policy on their performance and this can lead to a false sense of security.
- **Security is a learned behavior.** Security measures are often not intuitive and must be learned. Users must be trained and educated.
- **Expect the unexpected**. Policies will not be perfect. Keep policies simple to understand. Expect failures but weed out faults and loopholes before they cause breaches.
- **There is no perfect mousetrap**. No perfect policy exists. The environment, technology, applications, threats and systems change constantly. Review all policies regularly.

Policies alone can, therefore, not guarantee an improved security status of an organization. The one big problem that still exists is that people need to implement and manage the policies. The next part of the paper will define the elements of the Policy Dimension.

3 DEFINITIONS

Whitman defines a **policy** as 'a plan of action intended to influence and determine decisions, actions and other matters' (Whitman, Matford, 2004:194]. It will specify acceptable and unacceptable behavior. Policies are the organizational laws as they define acceptable behavior within the culture of an organization.

Standards are more detailed statements of what should be done to comply with the policy. The standards can be informal – de facto standards, or formal – de jure standards. It will be an agreed set of rules, procedures or conventions between parties in order to operate more uniformly and effectively. An example would be to use one e-mail application in the organization.

Procedures are plans, processes or operations that address the detail of how to perform a specific action. It typically answers questions of where, when and how, while policies answers who, what and why. Procedures are the lowest in the policy chain, as it will contain detailed systematic instructions to implement the statements in the policies, standards and guidelines.

Guidelines in the Information Security context refer to a set of recommended actions or policy statements that can be performed or adhered to in order to achieve a specific objective. Guidelines are laid down to remind users not to overlook or ignore specific security measures, even though the latter could be implemented in more than one way.

Baselines will provide the minimum-security requirements for a system, from which standards are developed. Standards specify how hardware / software should be used and enforce organization-wide uniformity when deploying technology and processes. Guidelines recommend actions when standards do not exist.

The standards and procedures of an organization are documented in the security standards and procedures manual of the organization. It is essential that policies are supported by applicable standards and procedures. Figure 1 will show the relationship between policies, standards and procedures

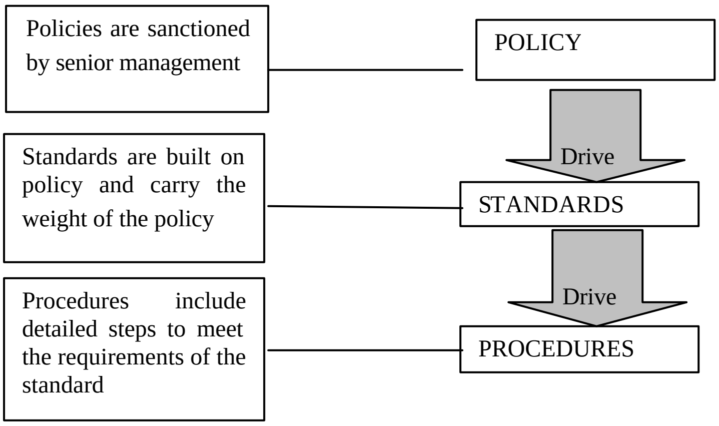

Policies are sanctioned by senior management
POLICY
Drive
Standards are built on policy and carry the weight of the policy
STANDARDS
Drive
Procedures include detailed steps to meet the requirements of the standard
PROCEDURES

Figure 1 The relationship between policies, standards and procedures (Whitman, Matford, 2003)

An Information Security policy provides a set of rules that protects the information and information assets of an organization in terms of Confidentiality, Availability and Integrity. The next part of the paper will discuss three types of Information Security policies.

4 TYPES OF POLICIES

From the literature studied, three general types of Information Security policies exist: General security policy, Issue-specific security policy and System-specific policies (Whitman, Matford, 2004), (Eloff, 2000).

The **general security policy** is defined at strategic management level of the organization. The policy must, therefore, be in line with the vision, mission and values of the organization. The strategic security objectives are important when formulating the general security policy. This policy will set the strategic direction, scope and tone for the security efforts in the organization. It is normally a short policy document that does not require frequent modifications.

The general policy will typically define the purpose, scope, constraints and applicability of a security program in the organization. Further, the policy assigns responsibilities to various areas of security, including systems administration, maintenance of policies and user education. The policy will also address legal compliance.

Every employee needs guidance in the normal routine tasks that he must perform everyday. Issue-specific policies will address specific issues of concern. It will address policy from a broad level, usually encompassing the entire organization. These would cover issues closer to computer networks, applications and data.

These policies will require frequent updates and should contain a statement of the position of the organisation on the specific issue. Typically issue-specific policies will include electronic mail, the use of the Internet, virus protection and detection and the use of photocopying equipment. Issue-specific policies are formalized documents prepared by the CIO (Chief Information Officer), signed off by the CEO (Chief Executive Officer), distributed to users and agreed to by the users in writing.

Issue-specific policies will not provide in-depth direction or information on how to configure a firewall but System-specific policies will fulfill this need.

System-specific policies are more detailed policies that can be used when configuring and maintaining systems. These policies are more focused and will address only one system and delve deeper into finer areas. System-specific policies are normally prepared by the IT department/CIO, and signed off by the CEO.

Security policies will not provide guidance on how to perform an action. Policies will only dictate that a certain goal must be reached. Underpinning policies are baselines, standards, guidelines and procedures that provide detailed information and directions on how to implement policies.

The relationships between policies, guidelines, standards and procedures are graphically represented by figure 2. The security program will be based on the general security policy, and supported by the issue-specific and system-specific policies. It is essential to ensure that system-specific policies and the issue-specific policies relate to the general security policy and that the standards, guidelines and procedures are in line with the applicable policy.

Policy management is essential once the policies have been developed and defined. The paper will not assess policy management. However the assessment model will check to see if a Policy Management system exists.

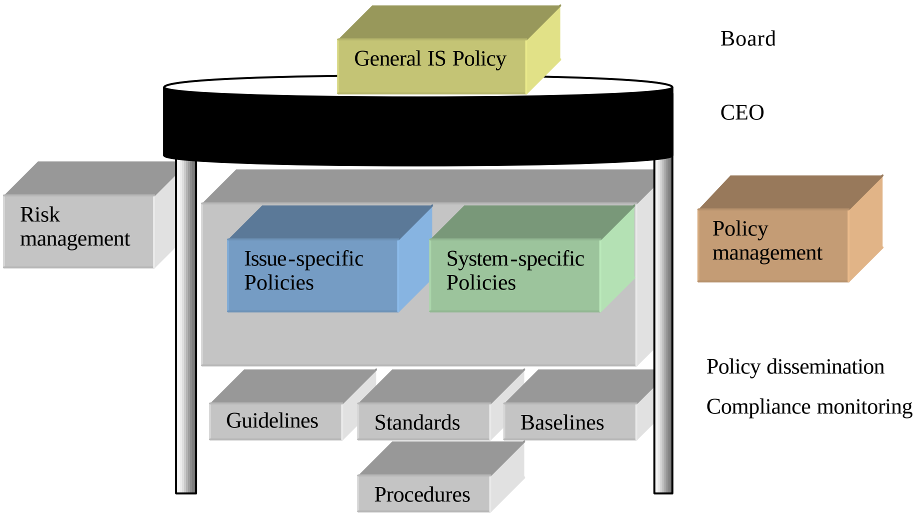


Figure 2 Policy framework (Mohan, 2003)

5 THE POLICY DIMENSION IN RELATION TO OTHER DIMENSIONS.

Von Solms described Information Security as a multi-dimensional discipline, which involves, in addition to technical security, other dimensions (Von Solms, 2001a). This paper will consider the following dimensions for Information Security: Corporate Governance, Policies, People, Technology, Compliance, Risk Management and Legal dimension. It is important to emphasize that no dimension can exist in isolation. All the dimensions are interrelated.

Corporate Governance relates to the responsibilities of the Board of Directors and top management of a company (Von Solms, 2001a). According to the King II report, they are responsible for securing and protecting the information assets in a company (King II, 2002]. Corporate Governance is divided into strategic and operational governance.

All internationally accepted best practices for Information Security Management accept the formulation of policies as the starting point to implement Information Security in an organization. An Information Security policy will provide a framework for selecting and implementing countermeasures against threats (Eloff, 2002a). The Policy dimension will cover all policies and propose that the organization should set up a policy framework.

The People dimension of Information Security is often neglected, but is crucial for the successful implementation of Information Security. It is essential to create and maintain an Information Security culture in the organization. This dimension includes user training and awareness programs.

To manage the risks in an organization is critical for survival. Risk Management is more than risk assessment, it includes the consultation and communication with the outside world to get the latest information on types of risks, risk assessment, how to treat risks and the implementation of the countermeasures to control the risks.

The legal dimension will incorporate the legal requirements as set out by government and other relevant business partners.

Compliance is an essential dimension. The purpose of this dimension is to determine the success of the implementation of the Information Security strategy in the organization. It includes the audit procedures of the organization.

All the above-mentioned dimensions must be implemented on a sound foundation of relevant technology. Technology will be either physical technology such as technical equipment like firewalls, or logical technology which includes access control software and database management systems and the implementation of networks.

The paper has identified the following relationships between the Policy dimension and the different other dimensions as illustrated in Figure 3.

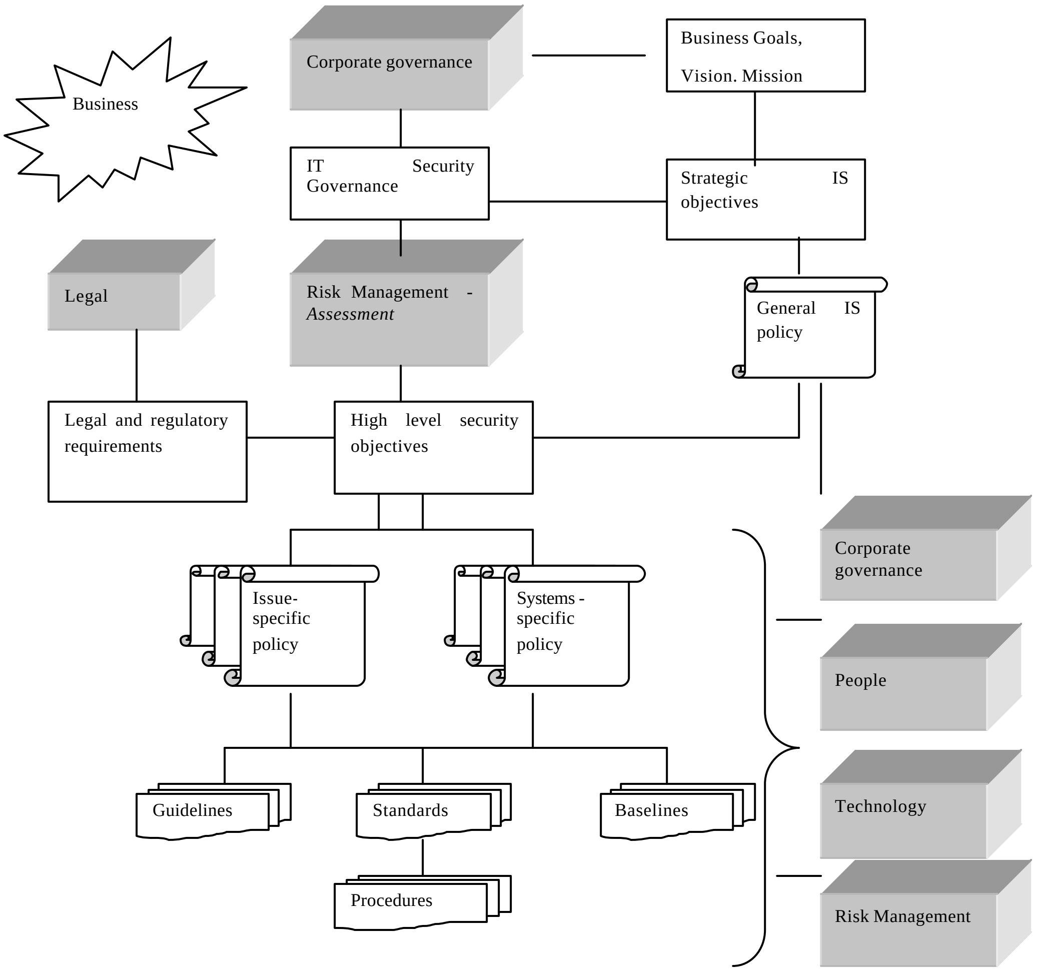


Figure 3 Policy dimension in relation to other dimensions

Business must exercise Corporate Governance. Top management will determine the strategic objectives and define the strategic security objectives of the organization. These objectives will revolve around Confidentiality, Availability and Integrity of information and information assets. The strategic objectives, as well as the results from the risk assessment exercise, will enable management to set up the General Information Security policy.

Legal requirements such as intellectual property and privacy of information must be identified. Policies should never contradict any law. The Risk assessment process will use the business goals and objectives of the organization and the strategic security objective to set up a set of high-level security objectives necessary for the organization.

Policies, issue-specific and system-specific, must be drafted to address the security objectives defined. A policy may address more than one objective and an objective can be addressed by more than one policy.

Each policy can have guidelines and/or standards with underlying procedures and/or baselines to enable the implementation of the policies.

The **deliverables** for the Policy Dimension are:

- a policy framework with
  - a General security policy,
  - a set of Issue-specific policies and
  - a set of System-specific policies, a collection of interrelated standards with associated procedures, guidelines and baselines
- a Policy Management System

These deliverables will be used by the People, Risk Management, Corporate Governance and Technology dimensions as indicated by figure 3. All the deliverables must be assessed to determine if all security issues have been covered.

The next part of the paper will propose a model to assess the Policy Dimension.

6 ASSESSING THE POLICY DIMENSION

The objective for an Information Security Policy is defined by the ISO17799 standard is:

> ***To provide management direction and support for Information security.***
>
> *Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an Information security policy across the organization.*

The author will adopt this definition as the main objective for the Policy Dimension. It is important to consider the objective when assessing the content of policies, guidelines and procedures.

When assessing the policy dimension it will be necessary to consider the following:

- The **completeness and relevance** of the policy set – Are all the risks and security objectives covered by the policies?
- The **format and content** of each policy – does it comply with best-practices?

- Do **underlying standards and procedures** exist to support the policy?
- Are the **policies managed** and distributed?

The author proposes the following **assessment model** for the Policy dimension. The assessment model will start at a macro-level and management will be guided on how to drill down to a micro-level during the assessment process.

The model proposes six high-level steps to assess the Policy Dimension. The assessor must perform the following steps:

Step 1: Obtain the existing policy set of the organization.

Step 2: Determine the completeness of the policy set (par. 6.1).

Step 3: Determine if the format of the existing policies is correct (par. 6.2).

Step 4: Determine if there are underlying standards and procedures supporting the existing policies.(par. 6.3).

Step 5: Determine if a policy management program exists.(par. 6.4).

Step 6: Determine the overall status of the Policy Dimension (par. 8).

The next part of the paper will discuss step 2 to step 5 of the assessment model.

6.1 STEP 2: DETERMINE THE COMPLETENESS OF THE POLICY SET.

During the risk assessment exercise, the organization must determine the security objectives for the organization. Based on these objectives an organization can determine which policies are necessary and important to the organization.

The author proposes a checklist of the most important policies in figure 4 to determine the completeness of the policy set. The list may not be complete, but is an indication of the most important policies as required by the SABS17799.

To assess the completeness of the policy set the assessor needs to:

1. complete the checklist in figure 4 by ***placing a tick in the appropriate importance column*** and the ***exist column*** for every policy,
2. ***determine the existence status*** of each policy by using the assessment criteria in figure 5. The status for a policy will be *Red or Yellow or Green* or Blue depending on the importance and existence of the policy in the organization and
3. ***indicate the existence status*** of each policy in the space provided on the checklist in figure 4

Importance			**Policy**	**Exist** **(Yes / No /** **Not sure)**	**Existence Status**			
High	**Low**	**N/A**			**Green**	**Yellow**	**Red**	**Blue**
			Access controls					
			Asset classification					
			Awareness policy					
			Business continuity					
			Clear desk					
			Compliance – Legal / policies					

			Copyright					
			E-Commerce					
			Education & Training					
			E-mail					
			General security Policy					
			Housekeeping					
			Incident handling					
			Information classification					
			Intellectual property					
			Internet usage					
			Licensing					
			Network access controls					
			Operations management					
			Personnel security					
			Physical security					
			Privacy					
			Remote access					
			Removal of property					
			Security organization					
			Systems development					
			Third party / outsourcing					
			Use of cryptographic controls					
			Virus protection					

Figure 4 Checklist to determine completeness of the policy set

Policy : X			
Importance	**Exist**	**Does not exist**	**Not sure**
Hi	Green 🟢	Red 🔴	Red 🔴
Low	Green 🟢	Yellow 🟡	Yellow 🟡
N/A	Blue 🔵	Blue 🔵	Blue 🔵

Figure 5 Criteria to assess the existence status of a policy

The **green** status will indicate that the policy exists. The **yellow** status will indicate that the policy does not exist but is of low strategic importance to the organization – it will be advisable to develop a policy. The **red** status will indicate that an important policy does not exist and immediate action should be taken to formulate the policy. The **blue** status will indicate that the organization does not need the specific policy.

If, for example, the outsourcing policy is of high importance but not documented, the status of the outsourcing policy will be RED. The assessor can determine which policies exist and which policies need to be developed

Management can use the checklist to get a bird's eye-view of the completeness of the current policy set. The existence status of each policy will be used in the final assessment of the Policy dimension in paragraph 8 of the paper.

After the completion of step 2 of the assessment model, the assessor has identified which policies exist and which policies must be developed. In step 3 of the assessment model, every existing policy will be assessed to determine if the format of the policy is correct and that sufficient content has been included.

6.2 Step 3: Assessing the format and content of each documented policy

Organizations develop policies, but it is essential that the format of all existing policies is correct and that the policies contain all the essential elements. A poorly formulated or incomplete policy can create ambiguity in the implementation and enforcement of a policy. Guidelines in best practices exist to guide the user on the format and content of different policies.

The assessment of the format and content will be on a conceptual level, as no specific policies will be discussed. The next part of the paper will discuss the typical layout of the general Information Security policy, issue-specific and system-specific policies. Checklists to assess the completeness and format of the existing policies are proposed.

6.2.1 General security policy format

The general security policy is a strategic, high-level policy. Management must approve the policy document. The document should be published and communicated to all individuals operating in the organization. It is important that the policy states management's commitment as well as a clear indication of management's approach to managing Information Security. According to the ISO17799 (SABS 17799) the policy should at least include:

- the definition of security, objectives and scope and indicate the importance of security,
- the statement of management's intent, supporting the goals and principles of Information Security,
- an explanation of the security policies, principles and standards and compliance requirements of particular importance to the organization, e.g.
    - Compliance with legal and contractual requirements
    - Security education requirements
    - Prevention and detection of malicious software
    - Business continuity management
    - Consequences of security policy violations , and
- a definition of responsibilities for Information Security Management including incident handling

To assess the format and completeness of the general security policy the assessor needs to:

1. complete the checklist in figure 6 by ***placing a tick in the Yes/No column***,
2. ***determine the format status*** of the general security policy by using the assessment criteria in figure 7. The status for the format of the policy will be *Green, Yellow or Red* and
3. ***indicate the format status*** of the policy in the space provided on the checklist in figure 6.

GENERAL SECURITY POLICY	Format Status		
	Red	Yellow	Green
Element	Yes / No	Comment	
Need for /Scope of Information Security			
Objectives of Information Security			
Management's intent / commitment			
Approval (Signature)			
Roles and responsibilities			
General elements Author Date of Policy Review date of policy			
Length style format			
Policy violations and disciplinary actions			
Monitoring and review			
User declaration and acknowledgement			
Security principles of importance to the organization			
Legal, regulatory and contractual compliance			
User awareness and training			
Virus protection and detection			
Business continuity planning			
Systems development and procurement			
Risk Management			
Personnel issues			
Outsourcing management			
Incident handling			
Information classification			
Access control			
Cross references			
Review			
Distribution			

Figure 6 Checklist for the format of general security policy

Policy: General Security Policy	
Number of Yes ticks	Format Status
< 20 (<70%)	Red 🔴
> 20 (>70%)	Yellow 🟡
28 (100%)	Green 🟢

Figure 7 Criteria to determine the status for the format of general IS policy

The **green** status will indicate that the policy has the correct format and contains all the required elements. The **yellow** status will indicate that the policy misses some elements and that the policy needs to be revised. The **red** status will indicate that the policy is poorly documented and immediate action should be taken to formulate the policy properly. The value of the status of the format status for the general security policy will be used in the final assessment of the Policy Dimension in paragraph 8 of the paper.

6.2.2 Issue- and system-specific policy format

The Issue-specific policies will concentrate on specific areas of current relevance such as disaster recovery, Internet usage or e-mail use. Typical components that should be included must be an issue policy statement, statement of the position of the organisation, applicability / roles and responsibilities as well as compliance.

System-specific policies are more focused, as it normally addresses one system or aspect. An example of a System-specific policy is password management policy in an organization. Assessing the format of both Issue-specific and System-specific policies can be done by using the checklist in figure 8.

To assess the format and completeness of an Issue-specific or System-specific policy the assessor needs to

1. complete the checklist in figure 8 by ***placing a tick in the Yes/No column***,
2. ***determine the format status*** of the policy by using the assessment criteria in figure 9. The status for the format of the policy will be Green or Yellow or Red and
3. ***indicate the format status*** of the policy in the space provided on the checklist in figure 8.

Policy Name: XXXX	Format Status		
	Red	Yellow	Green
Element	Yes / No	Comment	
Need for /Scope of Security			
Objectives of policy			
Management's intent / commitment			
Approval (Signature – manager)			
General elements Authors Date of policy Review date of policy			
Policy statement			
Statement of applicability: The who where how when to whom to what the policy applies			

Administration of the policy		
Policy violations and disciplinary actions		
Acknowledgement of policy (Signature user)		

Figure 8 Checklist for format of issue-specific and system-specific policies

Policy: X	
Number of Yes ticks	**Format Status**
(<70%)	Red 🔴
(>70%)	Yellow 🟡
(100%)	Green 🟢

Figure 9 Criteria to determine the format status of issue and system-specific policies

The green status will indicate that the policy has the correct format and contains all the required elements. The **yellow** status will indicate that the policy misses some elements and that the policy needs to be revised. The **red** status will indicate that the policy is poorly documented and immediate action should be taken to formulate the policy properly.

The value of the status of the format of each policy will be used in the final assessment to assess the Policy Dimension in paragraph 8 of the paper.

The assessor has now completed step 2 and step 3 of the assessment model. Step 3 has determined whether the existing policies are formatted correctly and contains the essential elements. In step 4 of the assessment model, the assessor must determine whether supporting standards, procedures, guidelines and baselines for every policy exist.

6.3 Step 4: Determine existence of supporting documentation

Every policy that exists should have supporting documentation. The assessor must determine what supporting documentation exists in terms of supporting policies, standards, procedures, guidelines or baselines. The purpose of this assessment will be to identify all the supporting documentation. It will not assess the completeness and applicability of the supporting documentation, but only whether it exists.

The author recommends that the organization should set up a list of all existing policies to indicate the existence of the supporting documentation as indicated in figure 10. Not all existing policies will have supporting documentation and the assessor needs to determine whether supporting documentation is necessary.

To assess the existence of supporting documentation the assessor needs to:

- **complete** the list of all policies with references to supporting documentation as set out in figure 10. (The assessor can use the list of policies as set out by figure 4),
- **determine the support status** of each policy by using the assessment criteria in figure 11. The support status of each policy will be Green or Yellow or Red or Blue and
- **indicate the support status** of the policy in the space provided on the checklist in figure 10

Policy	Reference to supporting documentation	Comment	Support Status
E-mail	Guideline 1.4		

Figure 10 List of policies with associated supporting documentation

Policy: X		
Supporting documentation	Necessary	Not applicable
Exist	Green 🟢	
Incomplete	Yellow 🟡	Blue 🔵
Does not exist	Red 🔴	Blue 🔵

Figure 11 Criteria to determine the status for supporting documentation

The green status will indicate that the policy has supporting documentation. The yellow status will indicate that some supporting documentation exists, but the documentation is insufficient. The red status will indicate that the policy has no supporting documentation, but supporting standards, procedures. is essential for this particular policy. The blue status indicates that the no documentation is necessary.

The assessor has now completed step 2, step 3 and step 4 of the assessment model. Step 4 has determined whether the existing policies have supporting standards, procedures, guidelines and baselines. The next step will be to determine if a policy management system exists.

6.4 Step 5: Policy management system

Step 5 will require the assessor to determine if a policy management system exists in the organization. The result will be either green or red, as a management system exists (green) or does not exist (red).

The next part of the paper will combine all the different status results obtained from the various assessments in steps 2 to 5 of the assessment model to propose a framework to assess the Policy Dimension (Step 6)

6.5 Step 6: Integrated assessment of Policy Dimension

The assessor has gathered the following information about:

1. The **completeness of the policy set –** indicating gaps that might exist where policies do not exist (paragraph 6.1)
2. The **format and content of existing** policies (paragraph 6.2)
3. The existing policies that have / need **supporting documentation** (policies, standards, procedures, guidelines and baselines) (paragraph 6.3)
4. The existence of a policy management system in an organization (paragraph 6.4)

The organization should organize the different policies, standards, procedures, guidelines and baselines in the organization in a structured way.

7 POLICY FRAMEWORK

Every organization should set up a policy framework to represent all the policies, standards, procedures, guidelines and baselines in the organization. The author recommends that the organization use the graphical representation of the policy framework as illustrated by figure 12.

The framework should include all policies, existing and missing policies, and all standards, procedures, guidelines and baselines.

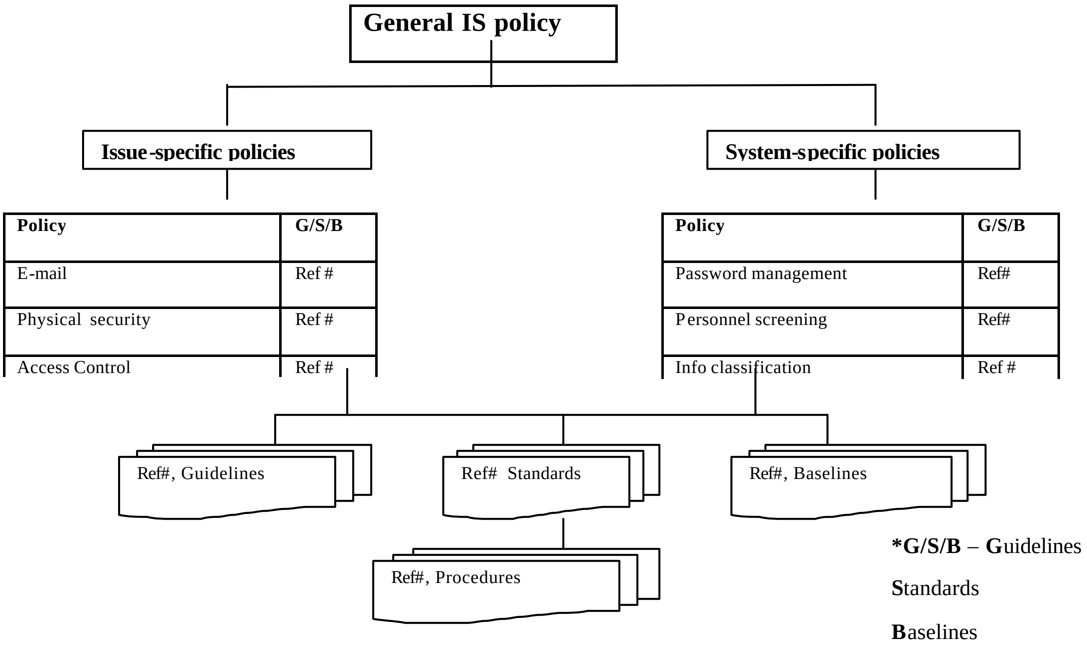


Figure 12 Policy framework

The assessor can now incorporate the different assessment status results to obtain a holistic, overall view of the status of the Policy Dimension.

8 INTEGRATED ASSESSMENT MODEL OF POLICY DIMENSION

The assessor should set up a complete list of all necessary policies in the organization using the framework and incorporate all the status results from the various assessments. Figure 13 is a snapshot of the list for illustration purposes. **To assess the overall status of each policy, the assessor needs to**

1. **make a list of all policies** as illustrated in figure 13. The assessor must use the list of necessary policies as identified in figure 4,
2. **include all status results** (existence, format, support) for each policy in the appropriate columns in figure 13,
3. **determine the overall status for each policy** by using the criteria in figure 14. The overall status of each policy will be Red or Yellow or Green or Blue and
4. **indicate the status value for each policy** in the space provided on the checklist in figure 13.

Status	Policy	Type	Format Status	Existence Status Completeness / Exist	Support Status: Supporting Policies, Standards etc.
	General IS policy	General	Green 🟢	Green 🟢	Green 🟢
	E-mail	Issue-specific	Green 🟢	Yellow 🟡	Green 🟢
	Info Classification	System-specific	Yellow 🟡	Green 🟢	Red 🔴

Figure 13 Assessed policies of organization

Status	Exist / Relevant	Format	Supporting S/P/G/B
🟢 Green	🟢	🟢	🟢 / 🔵
🟡 Yellow	🟢 / 🟡	🟢 / 🟡	🟢 / 🔵
🔴 Red	🔴		🟢 🔴 🔵
🔴 Red	🟢 / 🟡	🔴	🟢 🔴 🔵
🔴 Red	🟢 / 🟡	🟢 / 🟡	🔴 / 🔵
🔵 Blue	🔵	🟢 / 🟡 / 🔴	🟢 🔴 🔵

Figure 14 Assessment criteria for a overall policy status

The overall status of each policy will indicate the urgency of action that needs to be taken by management:

🔴 Red indicates that urgent action must be taken. A high priority policy has one or more of the following problems:

- The policy is not documented
- Problems exist with the completeness or format of the policy
- The policy is lacking supporting standards, procedures or guidelines

🟡 Yellow indicates that some action should be taken as there are still gaps in areas for example.

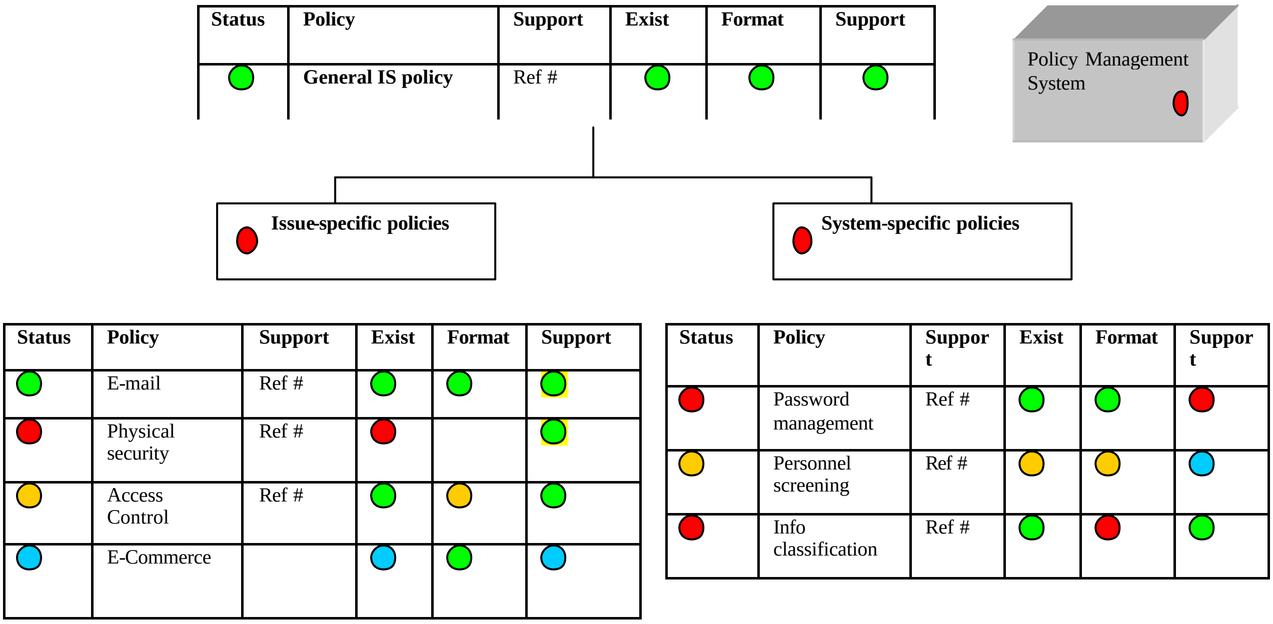
- The policy is not documented, but the policy is addressing a low priority issue to the organization
- Problems with the completeness or format of the policy

🟢 Green indicates that policy is fully in place - no action needs to be taken

🔵 Blue indicates that policy is no longer applicable to the organization and can be ignored – no action

The results obtained for the overall status of the individual policies in figure 13 can be added to the policy framework (figure 12) to enable management to get a visual view of the status of the Policy Dimension. The completed framework in figure 15 can be used as a model for the assessment of the Policy Dimension.

The assessor and management can determine the weak points in the Policy Dimension. They can prioritize the problem areas and address it in an appropriate way.



Status	Policy	Support	Exist	Format	Support
🟢	**General IS policy**	Ref #	🟢	🟢	🟢

Policy Management System 🔴

🔴 **Issue-specific policies**

🔴 **System-specific policies**

Status	Policy	Support	Exist	Format	Support
🟢	E-mail	Ref #	🟢	🟢	🟢
🔴	Physical security	Ref #	🔴		🟢
🟡	Access Control	Ref #	🟢	🟡	🟢
🔵	E-Commerce		🔵	🟢	🔵

Status	Policy	Suppor t	Exist	Format	Suppor t
🔴	Password management	Ref #	🟢	🟢	🔴
🟡	Personnel screening	Ref #	🟡	🟡	🔵
🔴	Info classification	Ref #	🟢	🔴	🟢

Figure 15 Integrated Model to assess the Policy Dimension

The author proposes a high-level overall assessment of the policy dimension. After completion of steps 1 to 5 of the assessment model the assessor can determine the current status of the entire dimension.

The status for each level in the policy dimension and the entire dimension can be determined. The status will be:

🟢	Green	If the status of all policies are green AND a Policy management system exists
🟡	Yellow	If >90% of policies are green and the remainder of the policies are yellow AND a Policy management system exists
🔴	Red:	If any policy is red OR No Policy management system exists

The assessment model has provided the assessor with a method to assess the Policy dimension systematically. The result of the assessment gives the assessor and management a clear indication of the overall status of the dimension.

9 SUMMARY

Policies that are well written, effectively communicated and consistently enforced will enable an organization to improve their security status. Without policies organizations runs the risk of being misunderstood by employees and/or business partners. It is also impossible to leverage disciplinary actions if a security violation occurs.

This paper has defined policies, standards, guidelines and procedures and indicated the relationship between them. The general security policy will provide intrinsic value and strategic advantage to the organization by improving the credibility among employees, customers and business partners. Issue-specific and System-specific policies will address specific issues in the organization. These policies should be supported by guidelines, standards, procedures and / or baselines.

When a security breach occurs, it is important to determine what caused the breach. The manager must determine if the policy has been defined properly or the guidelines and procedures were lacking.

The author has proposed a 6-step assessment model with appropriate assessment instruments to assess the Policy Dimension. The proposed assessment instruments includes various assessment checklists to assess the completeness of the policy set, the format of documented policies, whether adequate supporting documentation exist and whether a Policy Management system exists. The results of the above-mentioned assessments were combined to assess the entire Policy dimension.

10 REFERENCES

BUSINESS IT AFRICA. March 2001. *Security needs go beyond firewall.*

ELOFF JHP. 2002a. *What does international standards say on information security policies?.* IT Security workshop.

ELOFF JHP. 2002b. *Implementing an IT infrastructure to fulfill your organizational objectives*: IT security workshop.

ELOFF MM. 2000. *A Multi-dimensional model for Information Security Management*: PHD dissertation. RAU.

HUMAN FIREWALL COUNCIL. (2003). *Human firewall manifesto – a call to action. Website:* http://www.humanfirewall.org/rfmwm.htm, August 2003.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION. 1996. *Control Objectives for Information and Related Technologies.*

INTERNATIONAL STANDARDS ORGANIZATION. (1999). Website: http://www.iso.ch. Nov 1999.

KING II REPORT ON CORPORATE GOVERNANCE. 2000. Website: http://iodsa.co.za/lod%20Draft%20King%20Report.pdf, August 2003.

MOHAN F. *Policing system assets through Information Security policies*. Website: www.securesynergy.com. 15 August 2003

SABS ISO/IEC17799. (2001). SABS edition 11/ISO/IEC edition1, *South African Standard, Code of practice for Information Security Management*. South African Bureau of Standards.

TUDOR. *Information Security architecture*. (2001). Auerbach.

VON SOLMS SH. (2001a). Information Security. A multi-dimensional discipline, *Computers and Security*, volume 19, number 7. Elsevier.

VON SOLMS SH. (2001b) Corporate Governance and Information Security. *Computers and Security* Volume 20, number 3. Elsevier

WHITMAN M, MATFORD H. (2003). *Principles of Information Security.* Thompson Publishing.