

Policy as a Resource or “How You Can Get Rid of Several Binders”

Kent King, CISSP, CISA, CISM
Sterling Commerce

Sterling Commerce
An AT&T Company

Sterling Commerce at a Glance

- › Market leading solutions for:
 - Seamless and secure integration of key business processes
 - Streamlining the commerce lifecycle from selling to fulfillment to payments

- › \$630M in Revenue
- › 30,000 customers
- › 30 Years of Experience
- › An AT&T Company

Serving the Market Leaders



Market Penetration FORTUNE® Ranked Companies

95% of Fortune® 100 Companies

82% of Fortune® 500 Companies

Market Penetration in FORTUNE® 1000 Key Industries

93% Finance/Banking

79% Manufacturing

73% Retail

Source: Analysis of the 2006 FORTUNE 1000 and Sterling Commerce Revenues

Agenda

- › Policy in Your Organization
- › Standards for Policy Development
- › Making Policy a Resource
 - Framework Review
 - Build the Roadmap
 - Migration
 - Gap Analysis
- › Metrics
- › Keys to Success
- › Benefits & Lessons Learned

How Tough are Your Policies?

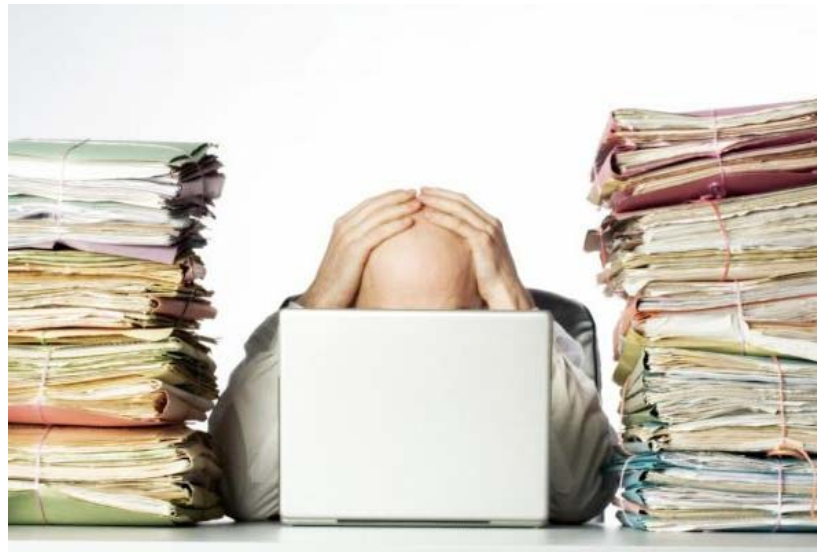


Policy in Your Organization

- › Is policy a large folder of documents?
- › Are policies created because of events?
- › Are policies created due to regulations?
- › Are policies limited by hardware & software?
- › Do you have a clear separation of policies and standards?
- › Have your policies and standards been audited?

Policy in Your Organization

- ⦿ Do you find users calling with policy questions because it is easier to ask than to look it up?
- ⦿ Do you believe anyone has read your policies?



Modern Policy Implementation

- › Make policies compliant with relevant standards or regulations
- › Have the ability to track and report user activity within policy framework
- › Decrease maintenance efforts
- › Better acquisition of products and services result from well defined standards



Standards for Policy Development

- › Most standards (ISO, NIST, COBIT) assume top down policy development
 - Many times policy is built bottom-up
- › Standards codify requirements
- › Customers recognize standards
- › Meet regulatory requirements
- › Faster audits reduce costs

Making Policy a Resource

Analysis

- Inventory existing documents
- Analyze structures
- Determine scope
- Customize application

Migration

- Extract from sources
- Format
- Import
- Configure application

Mapping

- Map controls to authoritative sources

Gap Analysis

- Create gap report
- Assess, prioritize and address deficiencies

Analysis

- › Inventory all existing policy documents
 - Locate current versions
 - Identify owners
- › Map inventory into target framework
 - You can explore other frameworks [here](#)
- › Create a framework diagram

Framework Review

- › Approximately 110 policies, standards, and supporting documents were inventoried
- › Considerable overlap found
 - Duplicate requirements in various documents
 - Separation of standards and policies
- › Gaps found to desired mapping

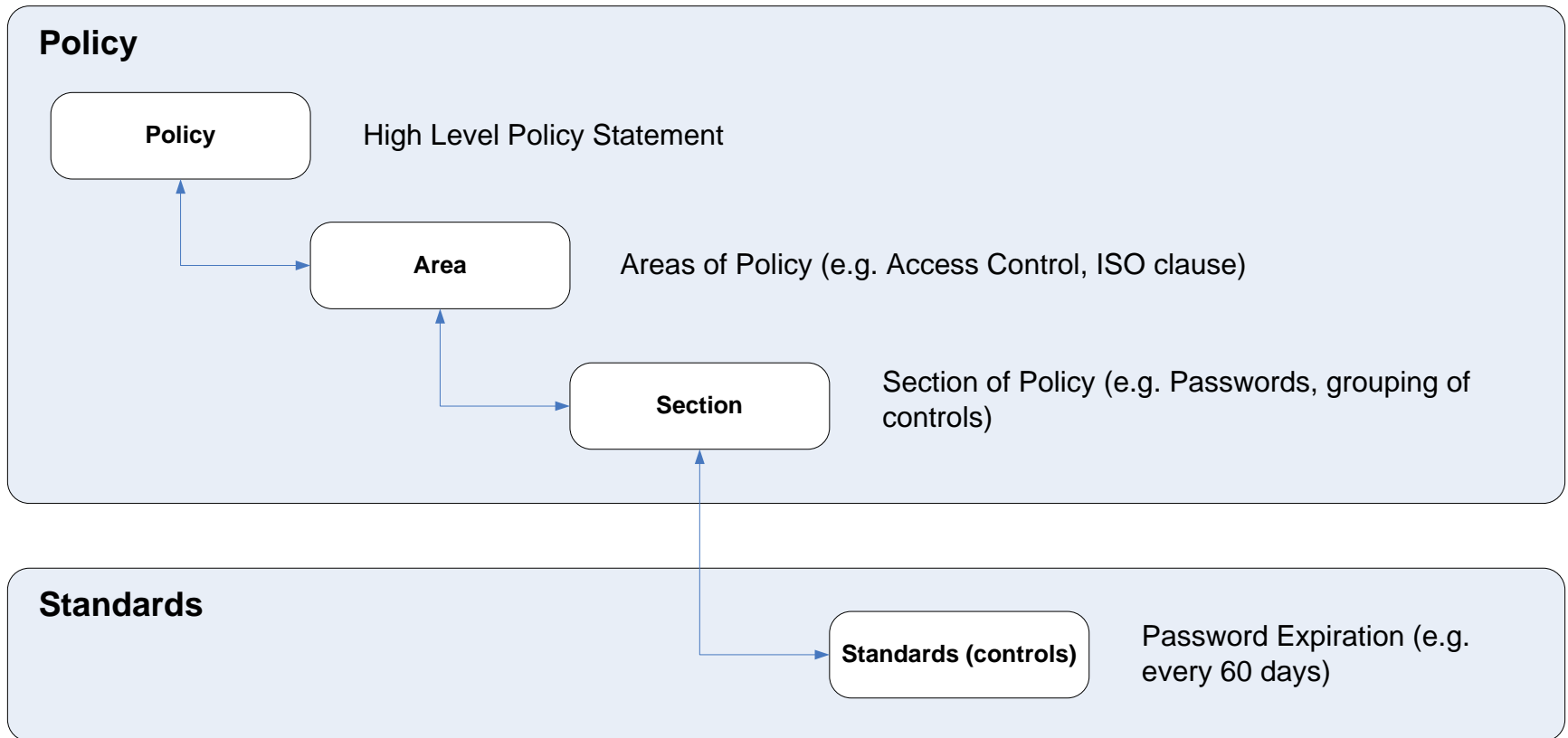
Framework Review

- › Don't be discouraged with diagram
 - Many “policy” documents include standards and even procedures
 - Many “standards” include policy level statements
 - Many documents will include multiple domains within the framework
- › Be aggressive in separating the overlap

Build the Roadmap

- › Consider how you classify policies
- › Create a policy schema
 - This will be dependent on the chosen framework
- › Decide how “atomic” the schema will be
 - Acceptable Use Standard
 - Password length requirement

Schema Overview



Policy Schema

Policy

Policy Name	<name>	Policy ID	<id>
Policy Purpose	<purpose>		
Policy Scope	<scope>		
Policy Statement	<statement>		
Key Points			
Area References			

Area

Area Name	<name>	Area ID	<id>
Area Objective	<objective>		
Area Overview	<overview>		
Area Purpose	<purpose>		
Area Scope			
Policy References	<references>	Section References	

Section

Section Name	<name>	Section ID	<id>
Section Objective	<objective>		
Area References	<references>		

Standard (Control) Schema

Standard Name	<name>		Standard ID	<id>
Grouping	<input type="checkbox"/> Access Authorization <input type="checkbox"/> Access Control Properties <input type="checkbox"/> Application / Systems Development <input type="checkbox"/> Business Continuity <input type="checkbox"/> Email <input type="checkbox"/> Encryption <input type="checkbox"/> Environmental Controls <input type="checkbox"/> External Networks <input type="checkbox"/> Fire and Water Protection <input type="checkbox"/> Firewall and other Network Protection Devices <input type="checkbox"/> Help Desk <input type="checkbox"/> Information / System Backup <input type="checkbox"/> Information Classification <input type="checkbox"/> Information Exchange <input type="checkbox"/> Information Handling <input type="checkbox"/> Information Ownership	<input type="checkbox"/> Information Security Responsibilities <input type="checkbox"/> Internal Audit <input type="checkbox"/> Intrusion Detection / Response <input type="checkbox"/> Legal and Regulatory Requirements <input type="checkbox"/> Management Commitment <input type="checkbox"/> Meetings and Conversations <input type="checkbox"/> Monitoring and Logging <input type="checkbox"/> Operational Controls <input type="checkbox"/> Passwords <input type="checkbox"/> Personnel Administration <input type="checkbox"/> Physical Security – Facilities <input type="checkbox"/> Physical Security – Information Resources <input type="checkbox"/> Privileged Access <input type="checkbox"/> Project Planning / Management	<input type="checkbox"/> Remote Access <input type="checkbox"/> Risk Assessments <input type="checkbox"/> Security Audits <input type="checkbox"/> Service Level Agreements <input type="checkbox"/> Technical Baselines <input type="checkbox"/> Testing and Validation <input type="checkbox"/> Third Party Service Providers <input type="checkbox"/> Third Party Software <input type="checkbox"/> Training and Awareness <input type="checkbox"/> User Authentication <input type="checkbox"/> User Identification <input type="checkbox"/> Virus (Malicious Code) Protection <input type="checkbox"/> Voice, Fax, Video Communications	
Classification	<input type="checkbox"/> Corrective <input type="checkbox"/> Detective <input type="checkbox"/> Preventive		Type	<input type="checkbox"/> Administrative <input type="checkbox"/> Application <input type="checkbox"/> Personnel <input type="checkbox"/> Physical <input type="checkbox"/> Technical
Audience	<input type="checkbox"/> Accounting <input type="checkbox"/> Business Development <input type="checkbox"/> Finance <input type="checkbox"/> Human Resources	<input type="checkbox"/> Information Security <input type="checkbox"/> Information Technology <input type="checkbox"/> Legal <input type="checkbox"/> Marketing	<input type="checkbox"/> Operations <input type="checkbox"/> Procurement <input type="checkbox"/> Public Affairs <input type="checkbox"/> Technology	
Statement	<statement>			
Policy	<references>		Authoritative Sources	

Migration

- › Finalize framework
- › Decide what will and will not be migrated
- › Determine what will be retired
- › Examples
 - Third Party Remote Access
 - Awareness Standards (New Hire, Ongoing, Third Party)

Migration

- › Resource intensive part of the effort
 - Break down old documents into components
 - Capture requirements/standards into new system
 - Rewrite maintained documents, updating links and references
- › Must watch for duplication at all levels
- › Many decisions on where things fall

New Policy Mapping

ISO 17799 Information Security Categories											
Risk Assessment & Treatment	Security Policy	Organization of Information Security	Asset Management	Human Resources Security	Physical and Environmental Security	Communications and Operations Management	Access Control	Systems Acquisition, Development and Maintenance	Security Incident Management	Business Continuity Management	Compliance
Information Security Policy											
Executive Endorsement											
Security Policies and Requirements											
					Data Center Access Policy			Change Management Policy			
Risk Management Standards	Administrative Security Standards	Information Classification Standards	Security Awareness Standards	Physical Security Standards	Operational Security Standards	Access Control Standards	Change Management Standards	Global Security SIRT Manual	Business Continuity Plan Standards	Compliance Standards	
		System Classification Standards			DMZ Architecture Standards		Service Realization Standards				
		U.S. Technology Use Policy			Security Logging Standards		Lab Security Standards				
		EMEA Technology Use Policy			TCP/IP Services Standards						
		APO Technology Use Policy			Bluetooth Security Standards						
		India Technology Use Policy			Mainframe Requirements						
					Unix Requirements						
					Windows Requirements						

Old & New Framework

ISO 17799 Information Security Categories											
Risk Assessment & Treatment	Security Policy	Organization of Information Security	Asset Management	Human Resources Security	Physical and Environmental Security	Communications and Operations Management	Access Control	Systems Acquisition, Development and Maintenance	Security Incident Management	Business Continuity Management	Compliance
High Level Policy & Requirements			Not Included in High Level Policy and Requirements			High Level Policy & Requirements			Not Included in High Level Policy and Requirements		
SCI Operating Practices 01 (OP01)									Not Included In OP01		SCI Operating Practices 01 (OP01)
Risk Management	Information Security Policy	MVS Requirements (Mainframe)	Asset Protection Policy	Workforce Member Training Policy	Personal Comp. Devices Security & Maint. Policy	MVS Requirements (Mainframe)			Incident Response	General Use & Disclosure Policy	
Risk Analysis & Risk Management Policy	Safeguarding Policy	General Networks & Remote Access	Asset Management Policy	Security Awareness Policy	Laptop Security Policy	General Networks & Remote Access		Service Realization	Threat Assessment & Monitoring Policy	Safeguarding Policy	
Vulnerability Assessment & Management Policy		Security Management Policy	Asset Identification & Classification Policy			Encryption & Authentication Using Cryptographic Functions		Change Management Policy	Global Security SIRT Manual	Prohibiting Retaliation Policy	
			Acceptable Use Policy			Unix Requirements				Software Licensing Enforcement Policy	
						Windows Requirements					
						External Entity Inter - Connections	Network Element Access Security				
						TCP/IP Services	RACF Governance Policy (Mainframe)				
						WLAN	Remote Access & Dialup Policy				
						Auditable Records					
						Security Gateways					
						Wireless Communications Policy					
						Network Storage Archive Retention Policy					
	Administrative Safeguards Standards	Information Classification Standard	New Hire Security Awareness Standard	Physical Security Awareness Standard	Bluetooth Security Standard	Change Management Standard	SIRT SLA	Business Continuity Plan Standard	Customer Management & Response Procedure		
	Vendor Management & Response Procedure	Desktop Asset Management Standard (OP01)	Ongoing Security Awareness Standard	Desktop Asset Management Standard (OP01)	DMZ Architecture (OP 01)	Access Control Standard	System & Application Deployment Standard	Incident Response Standard (OP01)	Storing Disaster Recovery Standard	Privacy Considerations Procedure	
		Information Classification Standard	Third Party Security Awareness Standard	Desktop /Laptop Security Standard (OP01)	Security Logging Standard (OP01)	Remote Access Control Standard	Applications Development Standard (OP01)				
		Internet Acceptable Use Standard		Physical Safeguards Standard	Secure Data Life Cycle Management Standard	Remote 3 rd Party Access Control Standard	Lab Security Standard (OP01)				
		Email Acceptable Use Standard		Workstation Use & Security Standard	Technical Safeguards Standard						
					Analog Line Security Std. (OP01)						
							Wireless Communications Standard				
							Non-SCI Connectivity Standard				

ISO											
Policies	Policies										
	1	2	3	4	5	6	7	8	9	10	11
Standards											

Gap Analysis

- › Gaps found between documents and desired mapping (ISO)
 - required improved classification standards
 - required improved asset management policy
 - required clarification of responsibility
- › Many gap items fell in two or more areas
 - Risk Management Policy



The Policy Portal



[Preferences](#) | [Reports](#) | [Help](#) | [Logout](#)

[Policy Management](#)



SCISP Portal

[Personalize](#)

[SCISP Policies](#) | [Search SCISP Policies](#) | [SCISP Standards](#) | [Search SCISP Standards](#) | [Submit an Incident Report](#)

February 18, 2009

Welcome to the SCISP Policy Center

Welcome to the Sterling Commerce Information Security Program (SCISP)

The SCISP Portal is your one stop shop for information security related policies, standards, and procedures. SCISP aligns with industry standards and the requirements of AT&T's Security Policies and Requirements (ASPR) Library.

Please see the [SCISP FAQ](#) for answers to common questions and the [brief tutorial](#). The [SCISP Overview](#) provides information on the structure, purpose, and objectives of SCISP.

To the right is Important information for workforce members. Below, quick access to all content in the SCISP repository.

Welcome, System General

Key Policies and Information

All workforce members must read and comply with the following:

- [SCISP Information Security Policy](#)
- Regional Technology Use Policies**
 Due to differences in local legal and regulatory requirements, technology use policies are specific to each region.
 - [SCISP Technology Use Policy \(APO\)](#)
 - [SCISP Technology Use Policy \(EMEA\)](#)
 - [SCISP Technology Use Policy \(U.S.\)](#)

Questions regarding any security requirements should be directed to [Global Security](#).

Browse the Entire SCISP Repository

Policy Name	Area Name	Section Name	
Information Security Policy			
SCISP Security Policies and Requirements	01 Risk Management	Risk Management Standards	
	02 Administrative Security	Administrative Security Standards	
	03 Asset Management		Sterling Commerce Information Classification and Protection Standards
			System Classification Standards
			Technology Use Policy (APO)
			Technology Use Policy (EMEA)
			Technology Use Policy (U.S.)
			Security Awareness Standards
	04 Human Resources Security	Physical Security Standards	
	05 Physical Security	AS/400 Requirements	
	06 Communications and Operations Management	Bluetooth Security Standards	

Other Ways to Find Requirements...

You can also browse [Control Standards by Grouping](#) (what they apply to) and [Control Standards by Audience](#) (who they are for)

[Sterling Commerce Global Information Security](#)

Click to Expand the Navigation Menu

Keys to Success

- › Know your application
 - If home grown – keep the developer around
 - If purchased – have at least one staff member certified on the product
- › Avoid embedded documents
- › Track and analyze exceptions
- › Limit use of “document view”

Cultural Challenges

- › Must break the habit of writing a new policy when something happens
- › Get users to use the system to research questions
- › System can show users why a policy exists (mapping to standards)
- › Provide new metrics to management
- › People seem to miss piles of documents

Benefits

- › Can generate pre-built reports for audit (SOX, PCI, etc.)
 - Reduce auditor on-site time
- › Can clearly see compliance with standards (ISO, NIST, etc.)
- › Improved exception management
 - Can use exceptions to drive awareness and policy changes
- › Issues became more external
 - Changes driven by regulatory compliance, not internally

More Benefits

- › Much better user questions
 - Be prepared for hard questions
- › Can find and address gaps rapidly
- › Make better policies and policy decisions
 - Much less “reactionary”
- › Easier to add/change and reference
- › Long term – Get HR/others to use system

Lessons Learned

- › Policies presented in a “standard” format may not always make sense to the end user
 - ISO, CoBit are designed for security and audit, not end users
- › Search tools continue to provide broad responses
- › Need to package and present “hot topics”
 - Access control, password standards
- › Major changes to policy review and approval processes

Questions?

Thank you!

Sterling Commerce
An AT&T Company