

Enterprise Security Policy Blueprint

Blueprint: Enterprise Security Policy Design

This blueprint outlines a step-by-step approach to an Enterprise Security Policy definition. It will need to be supported by additional activities which focus on the way the ESP is managed and administered once in place.

Analysis		Solution Design	
Business Requirements	Technical Requirements	Castle Defense System	Defense Planning
1- Business Model <ul style="list-style-type: none"> <input type="checkbox"/> Organization Model <input type="checkbox"/> Organization Goals <input type="checkbox"/> Products & Services <input type="checkbox"/> Geographic Scope <input type="checkbox"/> Organization Processes 2- Organization Structure <ul style="list-style-type: none"> <input type="checkbox"/> Management Model <input type="checkbox"/> Organization Structure <input type="checkbox"/> Vendors/Partner/ <input type="checkbox"/> Customer Relationships <input type="checkbox"/> Acquisition Plans (Business) 3- Organization Strategies <ul style="list-style-type: none"> <input type="checkbox"/> Business Priorities <input type="checkbox"/> Project Growth and Strategy <input type="checkbox"/> Legal Implications <input type="checkbox"/> Tolerance for Risk <input type="checkbox"/> TCO Objectives 4- IT Management <ul style="list-style-type: none"> <input type="checkbox"/> Centralized/Decentralized Management <input type="checkbox"/> Funding Model <input type="checkbox"/> Outsourcing/In-house? <input type="checkbox"/> Decision-making Process <input type="checkbox"/> Change Management Process 	1- Existing/Planned IT Environment <ul style="list-style-type: none"> <input type="checkbox"/> Organization size <input type="checkbox"/> Number of Users <input type="checkbox"/> Resources Location <input type="checkbox"/> Network Geographic Distribution and Links <input type="checkbox"/> Available Bandwidth <input type="checkbox"/> H/S Performance Requirements <input type="checkbox"/> Data Patterns <input type="checkbox"/> Network Roles and Responsibilities 2- Security Issues <ul style="list-style-type: none"> <input type="checkbox"/> Existing Systems and Applications <input type="checkbox"/> Technology Support Structure <input type="checkbox"/> IP Infrastructure <input type="checkbox"/> Authentication Services <input type="checkbox"/> Mobility Issues <input type="checkbox"/> Remote Workers <input type="checkbox"/> External Connections 	1- Critical Information <ul style="list-style-type: none"> <input type="checkbox"/> Data categorization <input type="checkbox"/> Application hardening 2- Physical Protection <ul style="list-style-type: none"> <input type="checkbox"/> Physical environment <input type="checkbox"/> Physical Control <input type="checkbox"/> Communications <input type="checkbox"/> Surveillance 3- Operation System Hardening <ul style="list-style-type: none"> <input type="checkbox"/> Security Configuration <input type="checkbox"/> Antivirus <input type="checkbox"/> General Active Directory Security <input type="checkbox"/> File System <input type="checkbox"/> Print System <input type="checkbox"/> .NET Framework Security <input type="checkbox"/> Internet Information Server <input type="checkbox"/> System Redundancy 4- Information Access <ul style="list-style-type: none"> <input type="checkbox"/> User Identification <input type="checkbox"/> Security Policies <input type="checkbox"/> Resource Access <input type="checkbox"/> Role-based Access Control <input type="checkbox"/> Access Auditing/ <input type="checkbox"/> Monitoring 5- External Access <ul style="list-style-type: none"> <input type="checkbox"/> Perimeter Networks <input type="checkbox"/> VPN <input type="checkbox"/> RADIUS/IAS <input type="checkbox"/> Public Key Infrastructure 	1- Threat Assessment <ul style="list-style-type: none"> <input type="checkbox"/> Attack Type Identification <input type="checkbox"/> Proactive Response Strategies <input type="checkbox"/> Reactive Response Strategies 2- Risk Assessment <ul style="list-style-type: none"> <input type="checkbox"/> Risk Identification <input type="checkbox"/> Risk Calculation <input type="checkbox"/> Risk Prioritization 3- User Awareness <ul style="list-style-type: none"> <input type="checkbox"/> Mandatory Training <input type="checkbox"/> Communication Plans <input type="checkbox"/> Technical Training Program 4- Monitoring Procedures <ul style="list-style-type: none"> <input type="checkbox"/> Events to Monitor <input type="checkbox"/> Monitoring Infrastructure 5- Attack Reaction Plans <ul style="list-style-type: none"> <input type="checkbox"/> Incident Response Team <input type="checkbox"/> Response Procedures <input type="checkbox"/> Escalation Procedures 6- Recovery Program <ul style="list-style-type: none"> <input type="checkbox"/> Core System Protection <input type="checkbox"/> Backup Systems <input type="checkbox"/> Restoration Procedures 7- Industry Watch <ul style="list-style-type: none"> <input type="checkbox"/> Security Event Watch <input type="checkbox"/> Virus Watch <input type="checkbox"/> New Product Watch <input type="checkbox"/> Product Upgrade Watch

Les Entreprises
Resolutions
Entreprises

[illegible]

By: _____