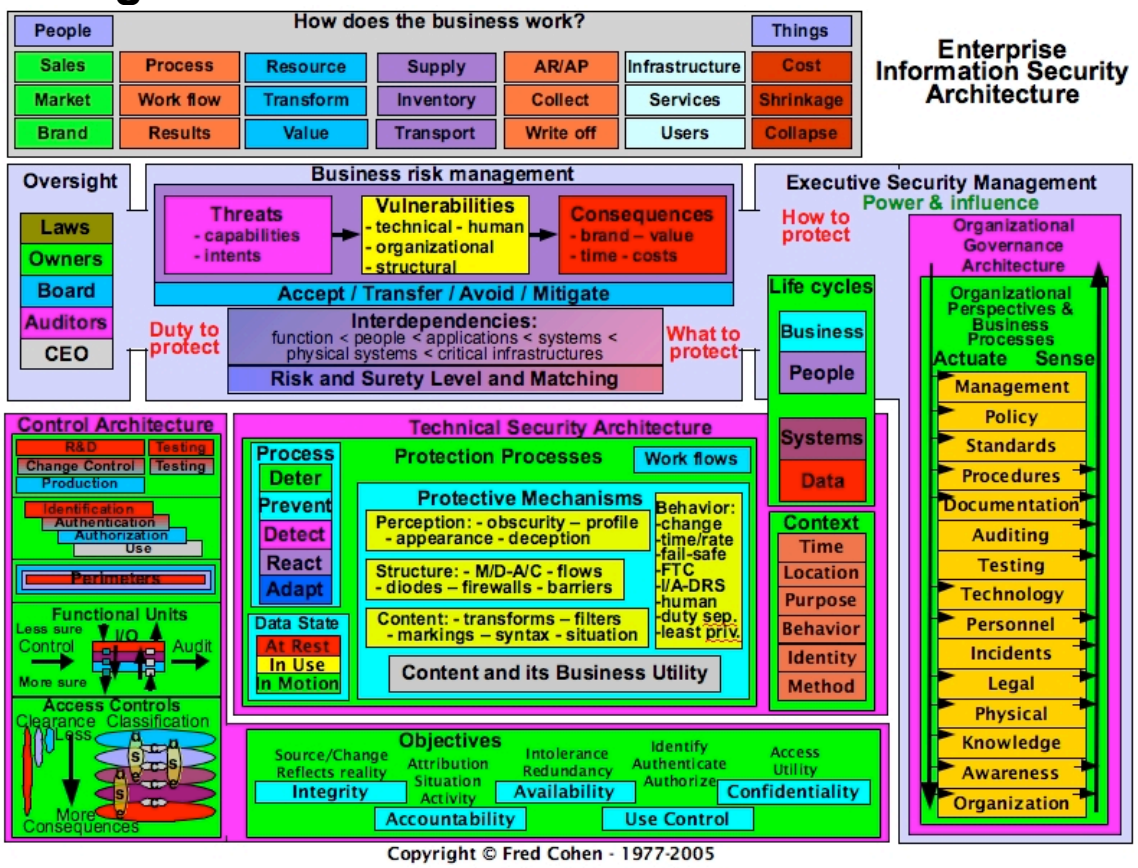
3 Program overview



Copyright © Fred Cohen - 1977-2005

3.1 Program structure

Rate the extent to which the overall program encompasses each issue identified from 0 to 10. Indicate short and long-term objectives for the program.

Area	*Current*	*Short-term*	*Long-term*
Business function			
Oversight defines duty to protect			
Business risk management			
Executive security management			
Organizational perspectives & feedback			
Control architecture			
Life cycle coverage			
Technical security architecture			
Process, context, and data state			
Protection mechanisms			
TOTAL: Add ratings and divide by 10			

3.2 Program goals

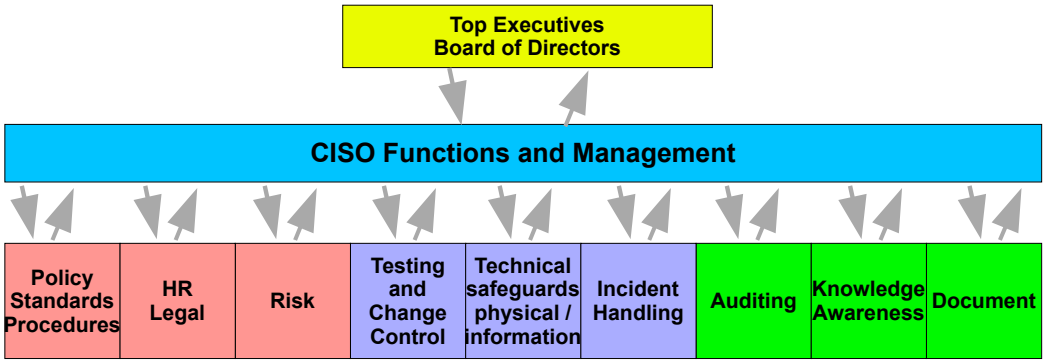
First specify program goals for the current period under the “Goal” column on a scale of 0 to 10. Next rate each area on a scale of 0 to 10 based on roll-up information from more in-depth assessments performed using checklists from throughout this booklet. Add up the goal and rating, divide the goal by the rating, multiply by 10, and produce an overall program metric for the period. Redo this on an annual basis.

Area	*Rate*	*Goal*
The overall program covers all of the areas in the chart.		
Information risk management is based on business risk management.		
Business processes enforce risk management with increasing rigor for increasing consequence.		
The information protection program is well attuned to how the business works and what is most important.		
Organizational structures provide the CISO influence or control over all organizational and business process areas.		
Objectives are quantified for the purposes of implementation.		
Life cycles are considered throughout the program and full life cycle coverage is applied in proportion to the need.		
The defense process balances deter, prevent, detect, react, and adapt so that the program is proactive while reactions are effective.		
Context is used with increasing accuracy as consequences increase.		
Data state drives and informs technical implementation.		
Safeguards are measured in terms of cost and utility		
Safeguards are selected to sever higher consequence attack graphs rather than to increase the general level of protection.		
There is an overall program architecture that facilitates achievement of these goals.		
There is a titled position for the CISO that is at the proper level and has adequate budget and access to get the job done.		
There is adequate top management support and visibility for the CISO function to be effective.		
TOTAL (add up each column)		
Program rating against goals (10 * rating total / goal total)		

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2	6	7	9	10

3.3 Organizational structure

Organizational structure provides a basis for overall program reach and viability.



3.3.1 People

List the CISO lead individual and the point of contact in other parts of the enterprise if the CISO team is not the lead on this particular issue. This is useful for assuring that the right people are informed and involved in appropriate meetings. If an area is missing or empty, the CISO should find an appropriate person to take the lead in this area, generate organizational mandate and budget to cover this area, and take charge of it.

Area	*Lead*	*POC*
Policy		
Standards		
Procedures		
HR		
Legal		
Risk management		
Change control & testing		
Technical safeguards		
Physical security		
Facilities		
Incident response		
Auditing		
Awareness and Knowledge		
Documentation		
Project manager		
Rating (number filled/1.5)		

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	10	10	10	10

3.3.2 Coverage

Coverage rates the extent to which the area is properly and adequately managed. For each area provide a rating from 0 to 10 based on roll-up information from more in-depth checklists or based on expert estimates.

Area	*Rate*
A policy, standards, and procedures group for information protection is in place and managed by the CISO function.	
HR and Legal departments interface effectively to the information protection function both at a technical level and at a management level.	
Risk management processes are effective and comprehensive.	
Change control & testing follow sound practices for applicable risk levels.	
Technical safeguards including informational and physical controls are commensurate with the risks they mitigate.	
Facilities personnel are highly supportive of protection requirements.	
Incident response detects all otherwise uncovered event sequences with significant potentially negative consequences in time to allow adequate mitigation through response.	
Auditing covers all facets of the information protection program and acts as an effective feedback system for managing the overall program.	
Awareness and knowledge levels are measured and found to be adequate to provide risk mitigation in the areas they are designed to cover.	
Documentation in support of the information protection program covers all regulatory and statutory requirements, policy requirements, and is effective at providing information for the operation of the program.	
TOTAL (add ratings and divide by 10)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2.5	5	6	7	9.5

3.3.3 Persuasion and organizational change

Rate the following areas from 0 to 10. Sum the ratings and divide by 3 for a total.

Item	*Rate*
Power and influence are mapped to determine candidate techniques for affecting organizational change	
The persuasion model is either formally used or internalized to develop effective presentations of material	
A formal organizational change management process is used to plan and carry out changes	
Overall rating (total / 3)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	N/A	2	6	10

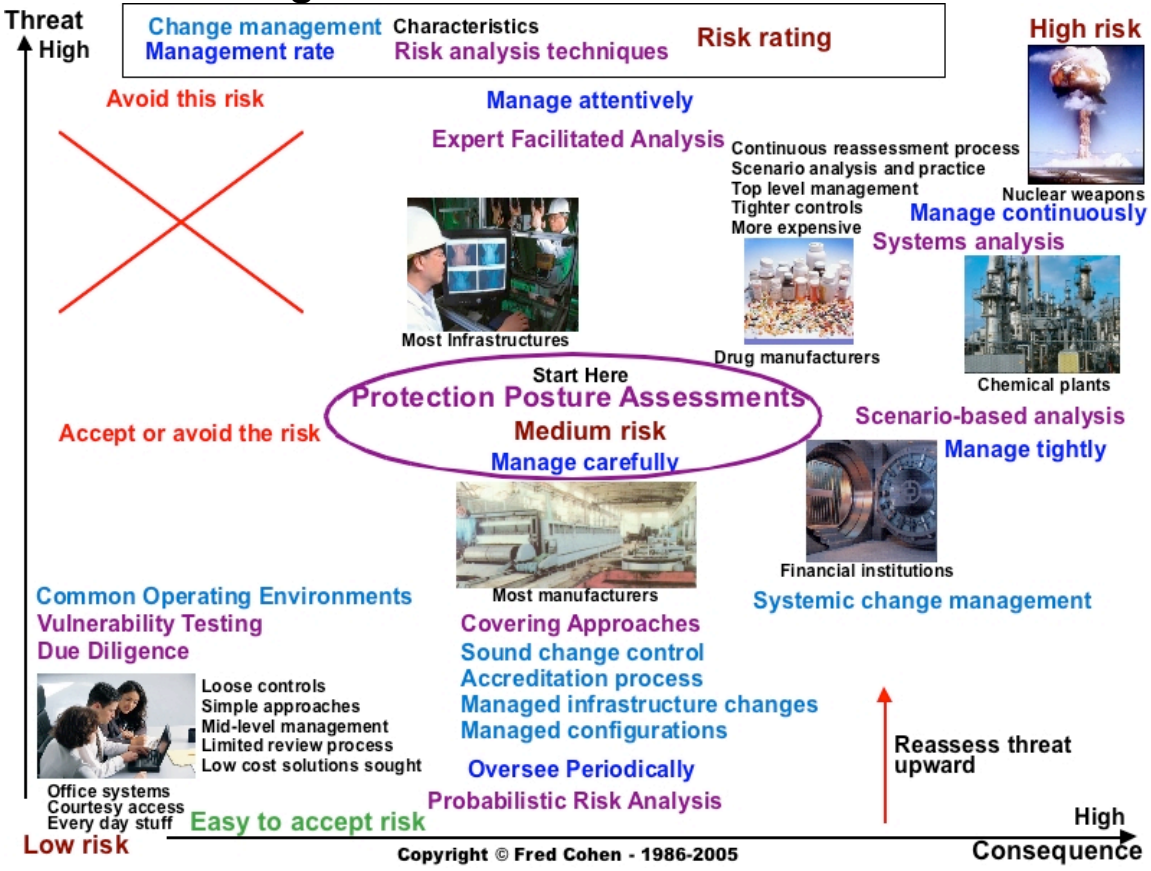
3.4 CISO performance

Rate each item from 0 to 10, sum and divide by 15 to generate an overall rating.

Item	*Rate*
People are trained, made aware, tracked, and managed	
Budgets are generated, justified, and used wisely.	
Effects by actuators allow the CISO to effectively influence events.	
Data generated by sensors including people and groups and reported to the CISO are adequate for control to be effective.	
Controls formed from feedback systems, technologies, procedures, processes, and a wide variety of other things within the power and direct or indirect influence of the CISO are effective at managing protection.	
Planning is done to cause the complex sequences of events involving people and systems to be properly coordinated.	
Strategy effectively translates the long-term vision of the enterprise and the CISO into plans that result in achieving the vision.	
Tactics effectively provide short-term event sequences that produce the functional behaviors desired in specific situations.	
Coordination effectively assures that the tactics as implemented remain within the desired set of future sequences.	
Politics successfully allow the CISO to control protection without creating unnecessary friction.	
Structure is effectively used and changed to provide direct and indirect control over behaviors and motivations.	
The enterprise rewards employees who show excellence in protection functions with raises and promotions.	
Punishments for poor security performance include poor performance reviews, sanctions, termination, and prosecution based on specifics.	
Security is included as a normal part of employee reviews and these are based on measurable performance metrics that are fed into the overall information protection program's measurement process.	
CISO communication is highly effective.	
Total / 15	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	8	6	9	10

3.5 Risk management



Area	*Y/N*
There is an identified risk management process.	
There is an identified risk management team.	
Policy dictates when risk management must make decisions.	
A protection posture assessment is done at least bi-annually.	
A threat assessment is done at least annually for non low risk systems.	
The threat assessment is the proper type for the risk levels involved.	
Vulnerability assessment is only done based on consequences and threats.	
Penetration testing is NOT done directly against high-valued systems.	
Low consequence, high threat systems are avoided.	
Threats are reassessed for low threat, high consequence systems?	
TOTAL (add the number of Yes answers)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	7	5	7	10

3.5.1 Surety and risk alignment

Rate each item from 0 to 10. Add ratings and divide by 6 to generate a total.

Area	*Rate*
Policy mandates that protection is commensurate with risk.	
A defined process exists for aligning risk with protection.	
The risk management process efficiently identifies medium and high risk areas and uses these distinctions to determine where to drill down.	
Surety processes and requirements are adequate to meet the protection needs for risks associated with those surety levels.	
Medium risk applications use at least medium surety systems.	
High risk applications use at least high surety systems.	
Total (add ratings and divide by 6)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	4	4	8	10

3.5.2 Consequences

Rate each item from 0 to 10. Add ratings and divide by 6 to generate a total.

Area	*Rate*
Top management defines thresholds for low, medium, and high risk.	
Additional or alternative thresholds are used for finer granularity.	
For high risk projects, detailed consequence analysis is done.	
Risk aggregation thresholds are considered in consequence analysis.	
Common mode failures are considered in consequence analysis.	
Radius requirements for risk aggregations are defined by top management.	
TOTAL (add ratings and divide by 6)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	5	3	6	9

3.5.3 Threats

Rate each item from 0 to 10. Add ratings and divide by 2 to generate a total.

Area	Rate
Threats are only analyzed in depth for medium and high risk systems.	
The assessment method selection identified below is used in determining assessment method.	
TOTAL (sum the rows and divide by 2)	

Assessment method	*Consequence*	*Time*	*Threat*	*Cost*
By type generic	Medium	Short	Medium	Low
By type, classes within groups	Medium-high	Medium	Medium-high	Medium
By type with classes and detailed high relevancy	Medium-high	Medium-long	Medium-high	High
Known vulnerability indications and warnings	Medium	Short	Low	Low
Detailed intelligence analysis	High	Long	High	High
Investigation-based	Medium-high	Medium	Medium-high	Medium-high

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	5	4	6	9

3.5.4 Vulnerabilities

Rate each item from 0 to 10. Add ratings and divide by 6 to generate a total.

Area	*Rate*
Vulnerability assessment is done for high risk systems.	
Vulnerability assessment is done for medium risk systems.	
Vulnerability scanners are used for low risk systems when cost effective.	
Penetration testing is done selectively against medium risk systems.	
Penetration testing against high risk systems is only done on test systems.	
Penetration testing is not done against low risk systems.	
TOTAL (sum the rows and divide by 6)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1	5	4	8	10

3.5.5 Balance

Rate each item from 0 to 10. Add ratings and divide by 8 to generate a total.

Area	*Rate*
A systematic approach determines how much redundancy is needed.	
Integrity requirements are weighed against costs to determine what does not need to be maintained accurately.	
Availability requirements are identified by project management on a case by case basis and metrics are used to determine how to achieve them.	
The criticality of confidentiality is assessed in determining the extent to which it is to be protected.	
Use control requirements are based on needs and security architecture.	
Accountability requirements are based on business drivers and the limits of attainable surety for the cost.	
Fail safe positions for all identified issues are determined by management.	
Risk management follows the table below.	
TOTAL (sum the rows and divide by 8)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0.5	6	4	7.5	9.5

Acceptable	Transferable	Reducible	Action
No	No	No	Do not engage in this—avoid the risk
No	No	Yes	Propose reduction and re-evaluate
No	Yes	No	Insure or avoid the risk
No	Yes	Yes	Balance reduction with insurance cost
Yes	No	No	Accept or avoid the risk
Yes	No	Yes	Balance reduction vs. acceptance cost
Yes	Yes	No	Accept or avoid the risk
Yes	Yes	Yes	Balance all three and optimize

3.5.6 Process

Rate each item from 0 to 10. Add ratings and divide by 9 to generate a total.

Area	*Rate*
A well-defined risk management process is in place.	
The process starts with consequences.	
Threats are assessed in increased detail for medium or high consequences.	
Vulnerabilities are viewed for paths from threats to non-low consequences.	
Approaches are used per the risk management figure above.	
Risk management is repeated at rates indicated by the table below.	
Risk management determines when risks are to be accepted, avoided, transferred, and mitigated.	
Policy elements are mapped into risk management processes.	
A schedule for risk management is used to assure program function.	
TOTAL (sum the rows and divide by 9)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2.5	5	5	7	9.5

	Low Consequence	Medium Consequence	High Consequence
Low Threat	Mid-level mgmt updates annually	6-month review cycle, top mgmt update annually	Should not occur – threats are higher
Medium Threat	Mid-level mgmt update 9-12 months	3-9-month review cycle, top mgmt update quarterly	Continuous top mgmt updates monthly
High Threat	Should not occur—not worth operating	3-6-month review cycle, top mgmt update quarterly	Continuous top mgmt updates monthly

3.5.7 Roll-up

Enter summary totals from the previous tables. Sum and divide by 7 for an overall rating for risk management.

Area	*Rate*
Initial overall rating	

Area	Rate
Surety and risk alignment	
Consequences	
Threats	
Vulnerabilities	
Balance	
Process	
TOTAL (sum the rows and divide by 7)	

Startup	Diligence	Typical	Excellent	Best
0.5	5.2	4.2	7.1	9.6

3.5.8 Interdependencies

Rate the extent to which risk management analyzes dependencies on and of each item from 0 to 10. Sum all ratings and divide by 32 for the overall rating.

Item	Rate	Item	Rate
Business utility		Users	
Administrators		Support personnel	
Application programs		Data files	
Input and output systems		Systems infrastructures	
Operating systems		Code libraries	
Configurations		Application infrastructures	
Domain name services		Identity management systems	
Back-end processing facilities		Protocols	
Physical infrastructures		Computing platforms	
Networks		Wires	
Routing protocols		Accessibility	
Power		Cooling	
Heat		Air	
Communications		Government & political stability	
Environment condition & control		Supplies	
People in the society		Safety and health of people	
		TOTAL (sum all ratings / 32)	

Rate each item from 0 to 10. Sum ratings and divide by 4. Add the previous rating and divide by 2 for an overall rating.

Item	Rate
No single points of business failure exist.	
Single points of system failure are identified & mitigated appropriate to risk.	
Common mode failures are evaluated and limited in scope.	
Radius of effects are analyzed for threats and consequences to assure that adequate physical separation is applied for redundancy.	
TOTAL (sum ratings and divide by 4)	
OVERALL RATING (add this total to the previous total and divide by 2)	

Startup	Diligence	Typical	Excellent	Best
1	5	4	7	10

3.6 Interdependencies and technologies

Interdependencies are often ignored resulting in large-scale harm from seemingly small events. This notion of unintended consequences is understood this way.

3.6.1 Interdependencies

Rate from 0 to 10 the extent to which each area is checked for dependencies in the analysis of risk and the computation of ratings for consequence and surety.

Area	*Rate*
Business utility	
People	
Applications	
System infrastructure	
Application infrastructure	
Physical infrastructure	
Critical infrastructure	
TOTAL (sum the ratings and divide by 7)	

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
2.5	5	6	7	9.5

3.6.2 Risk aggregation

Rate the following areas from 0 to 10 in terms of the extent to which they are understood and assessed as part of the risk management process.

Item	***Rate***
Management defined consequence thresholds are used for risk levels.	
Risk aggregation is analyzed in low risk environments.	
Risk aggregation is analyzed in medium risk environments.	
Risk aggregation is analyzed in high risk environments.	
Aggregated risk is mitigated by increasing surety levels.	
Aggregated risk is mitigated by partitioning the risk area.	
TOTAL (sum the ratings and divide by 6)	

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
2.5	5	6	7	9.5

3.6.3 Technologies

Under risk management (R) indicate which surety levels are associated with each of these requirements. For each of low (L), medium (M), and high (H) surety levels, rate from 0 to 10 the extent to which each statement is true. Add the "L"s, "M"s, and "H"s under R and write each of them down. Add the total of those and write them under the TOTAL for R. Sum the numbers under each of L, M, and H and write them down under as TOTAL. For ratings divide each of the sums for L, M, and H by their respective totals and multiply by 10. Sum them under R.

Area	*R*	*L*	*M*	*H*
Integrity is protected by source authentication				
Integrity is protected by change controls				
Integrity is protected by consistency checks				
Integrity is protected by independent validation				
Integrity is protected by cryptographic checksums				
Availability is protected by high quality systems designs				
Availability is protected by strong maintenance processes				
Availability is protected by strong change controls				
Availability is protected by redundancy				
Confidentiality is protected by access controls				
Confidentiality is protected by encryption				
Confidentiality is protected by network separation				
Use is controlled by strong authentication				
Use is controlled using identity management infrastructure				
Use is controlled by roles and rules				
Use is controlled by strong authorization limitations				
Use is controlled by redundant control mechanisms				
Accountability is facilitated by independent audits				
Accountability is enhanced by strong attributions to individuals				
Accountability is associated with all activities				
Accountability is assured by comprehensive audit trails				
TOTAL (For L= For M= For H=)				
RATING (Total for each of L, M, H / total Rs for L, M, H)				

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2.5	5	6	7	9.5

3.7 The CISO Budget Source and Cost Chart

This table is designed to provide a roll-up of overall protection-related costs for their enterprise.

Area	Budget source	Annual Costs	Hidden costs
Security management			
Policy			
Standards			
Procedures			
Documentation			
Security Auditing			
Protection Testing			
Technology			
Personnel (training)			
Incident handling			
Legal			
Physical			
Knowledge			
Awareness			
Organizational			
Business life cycles			
People life cycles			
System life cycles			
Data life cycles			
Deterrence			
Prevention			
Detection			
Reaction			
Adaptation			
Integrity			
Availability			
Confidentiality			
Use control			
Accountability			
Risk management			
Insurance (transfer)			
Losses			
Mitigation			
Public relations			
Brand			
TOTALS	N/A		