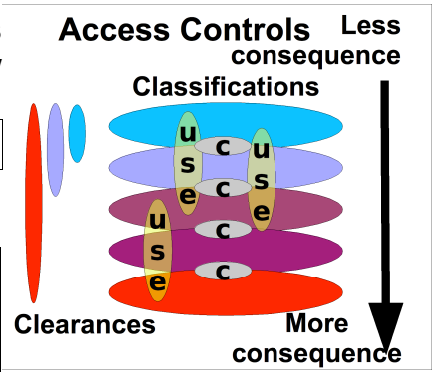
8.2 Access controls

Identify goal state rated from 0 to 10 then assess current ratings. Add up final ratings in charts below (20 of them) and divide by 20 for overall rating:

Total architecture rating (sum totals / 20)	



8.2.1 Control structure

Objective	*Rate*	*Goal*
An enterprise information content control structure is defined.		
It includes clearances, classifications, uses, need to use, and controls		

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	5	6	7	10

8.2.2 Clearances

Specify the situation for each issue as Yes/No (or True/False) then add results in the totals area.

Issue	*Y/N*
Only human beings get clearances.	
There is a clearance associated with “not yet rated”.	
There is a clearance associated with “general purpose use”	
There a clearance associated with “external users from the Internet”.	
Every legitimate user has an identified clearance rating.	
There is a defined clearance process associated with each clearance type.	
The clearance process is adequate based on risk management.	
Clearances get reviewed periodically based on risk management periods.	
The clearance process is audited internally.	
The clearance process is reviewed or audited externally.	
TOTAL number of YES answers (out of 10)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
0	3	4	7	10

8.2.3 Consequences

Rate each area from 0 to 10. Add up ratings and divide by 3.

Area	Rate
Consequences form the basis for the classification system.	
Risk aggregation is used as a basis to limit use.	
Separation mechanisms are based on consequences.	
TOTAL (add up ratings and divide by 3)	

Startup	Diligence	Typical	Excellent	Best
1	6	6	8	10

8.2.4 Classifications

For each area in each of low (L), medium (M), and high (H) consequence columns, indicate yes/no (Y/N). Specify the risk management requirement as L, M, or H for each entry under R to indicate the level at which this area must be covered by policy. Add up the number of L, M, and H areas indicated by R in the "desired" row. Add up the number of Yes answers in each column and total in the "achieved" row. Add up the number of Yes answers achieved but not desired in the "excessive" row. Subtract twice the "excessive" number from the "achieved" number, divide by the "desired" number, and multiply by 10 to generate the rating for each column.

Area	R	L	M	H
Risk management requirements for classification of content exist.				
All content gets a classification at inception.				
Classification is tracked throughout content life cycles.				
All functional components have use types specified.				
All functional components have surety ratings.				
All functional components are rated for use by clearance				
All functional components have time of day limitations.				
All functional components have location limitations?				
All functional components have "need to use" limitations?				
Mechanism prevent access when classification exceeds clearance.				
Mechanisms prevent access when user use is not appropriate to content or system use category.				
Desired total for each risk level				
Achieved total for each risk level				
Excessive total for each risk level				
RATING: ((Achieved – (2*Excessive)) / Desired) * 10				

Risk	Startup	Diligence	Typical	Excellent	Best
Low	0	5	5	7	10
Medium	1	5	6	8	10
High	1	5	6	8	10

8.2.5 Separation mechanisms

8.2.5.1 Separation Basics

Rate each issue from 0-10, sum the ratings and divide by 3.

Issue	*Rate*
Separation mechanisms between classifications prevent mixing of content except through controls.	
Separation mechanisms within classifications adequately limit mixing of content and control based on use to meet risk management requirements.	
Separation mechanisms adequately limit interaction of control and content flows to meet risk management requirements.	
TOTAL (total and divide by 3)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
2	5	6	9	10

8.2.5.2 Separation in more detail

For each area, indicate yes/no (Y/N) for implementation in low (L), medium (M), and high (H) consequence and specify the risk management requirement (R). Add the number of areas compliance is desired for each consequence and enter into “desired” row. Count Yes answers in each column and total in “achieved”. Count Yes answers achieved but not desired with substantial cost in “excessive”. Subtract twice “excessive” from “achieved” and divide by “desired” in each column and multiply by 10 to generate the rating.

Issue	*R*	*L*	*M*	*H*
There is adequate separation between surety levels to eliminate interference between them.				
There are adequate protective barriers to increase the surety level between zones in the control scheme.				
Control, audit, and data flows are separated for medium and high surety levels.				
Audit is separated from control and data for all surety levels.				
Separation between protective zones meet the requirements of those zones.				
There segregation of duties between control, functions, and audit.				
Risk aggregation considered in the separation of systems at each surety level.				

Issue	R	L	M	H
Desired total for each risk level				
Achieved total for each risk level				
Excessive total for each risk level				
RATING: ((Achieved – (2*Excessive)) / Desired) * 10				

Risk	Startup	Diligence	Typical	Excellent	Best
Low	0	5	5	7	10
Medium	1	5	6	8	10
High	1	5	6	8	10