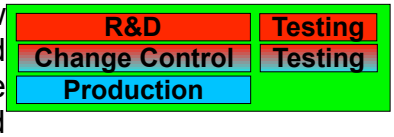
8.6 Change control and testing

8.6.1 Change control



For each area, indicate Y/N for implementation in low (L), medium (M), and high (H) consequences, and specify the risk management requirement (R) for the level. Count the areas in which compliance is desired for each consequence level and enter into “desired”. 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*
Risk management dictates specific change control requirements.				
The production environment is only for applications, and is never used for programming tasks.				
The only path for program changes to the production environment goes through change control.				
Change control can not change anything sent to it from R&D				
Change control can only pass information to production that has entered from R&D and can only pass whole components and verification codes such as checksums, and not parts of components.				
Only source code is passed to change control.				
Binary files are generated from source in the production environment.				
Binaries in production are verified against R&D and CC checksums.				
Source codes are verified in production against those found in change control and R&D.				
Changes may only enter the change control area based on an approved change request with a specific goal.				
The actual change is verified by change control to be appropriate to the goal.				
No unnecessary program or data changes are permitted.				
The operation of the programs and changes and the effects of the change must be both clear and obvious.				
Changes must also pass tests on sample data in order to assure that they actually work.				

Issue	*R*	*L*	*M*	*H*
All information interpreted by Turing capable mechanisms goes through change control				
Emergency bypasses to change control are rare and audited in detail immediately after the change.				
Emergency bypasses to change control always involve a change that has been previously tested.				
Change control retains regression information to allow previous versions to be reasserted in case changes cause problems.				
The change mechanism operates through the control plane and is independent of the data stream				
All change control actions are audited and audits review these changes for correctness against all criteria.				
Regression testing is undertaken in R&D and all regression detected faults are fixed before sending code to change control.				
Regression testing is done in change control to verify regression testing in R&D.				
Desired total for each risk level				
Achieved total for each risk level				
Excessive total for each risk level				
RATING: ((Achieved – (2*Excessive)) / Desired) * 10				

8.6.2 Change control overall

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

Area	*Rate*
Changes to production systems are throughly tested.	
Changes to production systems are verified to meet the need.	
Changes to production systems are verified to contain no unnecessary or inappropriate hardware or software.	
Changes to production systems are verified to work properly on test data.	
Changes to production systems can be reverted to previous states in a timely fashion.	
Changes to production systems are verified to operate properly under emergency conditions.	
Verification and testing processes involve administrative and technical approval.	
A tracking process is used to verify that change control operates correctly.	

Area	Rate
Disaster recovery and business continuity planning programs use change control at the level of surety of the systems they cover.	
TOTAL (add ratings and divide by 9 for a total)	

Startup	Diligence	Typical	Excellent	Best
2	5	6	8	10

8.6.3 Testing

Rate each issue from 0 to 10 and sum the ratings and divide by 21 for a total.

Area	Issue	Rate
Fault models	Basic phenomenological models of faults that occur and how they are manifested to the observer are used.	
	These fault models are validated by empirical evidence.	
	These fault models are used as a basis for measurements in the protection testing process.	
Coverage	Coverage is used to measure protection testing efforts.	
	Coverage levels are defined as objectives of protection testing.	
	100% coverage is required for all fault models in high surety systems.	
	100% coverage is required for non-accepted or transferred fault models in medium surety systems.	
Regression	Testing against all known historical weaknesses is used before changes are sent to change control.	
	Testing against all known historical weaknesses is verified as part of change control.	
	Failure to pass regression tests in change control is reflected in personnel action against the author of the change.	
Periodic	Periodic testing of all non-high risk systems is undertaken.	
	Periods between testing are based on risk levels.	
	Risk management dictates testing periodicity.	
	Test periods reflect change rates and system complexity.	
	Periodic testing of high-risk test systems is undertaken.	

Area	*Issue*	*Rate*
Change	Testing is required for medium and high risk systems undergoing any hardware or software changes.	
	Testing integrates with the enterprise change management system.	
Blind	Conditions for blind testing are defined and applied uniformly.	
	Proper controls over blind testing and responses are in place.	
Planned	Planned tests have well defined performance requirements and circumstances.	
	Disaster recovery and business continuity planning programs are tested thoroughly at least yearly.	
TOTAL	Add ratings and divide by 21 for a total	

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
1.5	5	6	8	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