9.5 Work Flow

Rate each item from 0 to 10. Sum the ratings and divide by 13 for a total rating.

Item	*Rate*
Protection process is implemented in terms of a set of defined work flows.	
Work flows are defined and documented in writing.	
Work flows are used to assure that work gets done in the proper sequence.	
Work flows are used to assure that approvals are properly undertaken prior to actions.	
Work flows are used to automate provisioning for automatable work flows like adding user identities based on roles and similar functions, only up to management specified risk aggregation limits.	
Work flows are used to document the protection process,	
Work flows are used to verify proper operation of the protection program and its elements.	
Work flows are used to reduce the work load for audit.	
Work flows are used to support protection process improvement.	
Work flow automation is limited to limit risk aggregation.	
Identity management solutions are limited in their scope to limit risk aggregation to executive management specified levels.	
Surety levels associated with work flow systems are commensurate with the risks they aggregate.	
Attacks against work flow causing all access to cease, granting of access to unauthorized individuals, destroy information functions, disrupting operations in automated manufacturing or processing facilities, and other similar attacks are considered in the implementation of work flow systems.	
TOTAL (sum the ratings and divide by 13)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10

9.5.1 Work to be done

Rate each item from 0 to 10. Sum the ratings and divide by 5 for a total rating.

Item	*Rate*
Work to be done is codified in work flow systems whether manually or automatically implemented.	
For the small or medium sized businesses, or for small business units within enterprises, checklists for many of the common functions are used where automation is not readily available.	
For large enterprises some level of automation is used to reduce costs while improving the effectiveness of provisioning and similar functions.	
Checklists and automation are audited to assure that they reflects the proper work to be done.	

Item	*Rate*
Execution of the work is verified by review and audit periodically.	
TOTAL (sum the ratings and divide by 5)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10

9.5.2 Process for completion and options

Rate each item from 0 to 10. Sum the ratings and divide by 8 for a total rating.

Item	*Rate*
For each item of work to be done a process for completion is defined	
For each item of work to be done the conditions for its invocation are specified.	
For each item of work to be done the times associated with different actions to be undertaken is specified and verified.	
For each item of work to be done the primary and auxiliary contacts for performing the identified tasks are identified.	
For each item of work to be done the optional processes for emergency, standard, and exceptional conditions including appeals processes and overrides are defined.	
For each item of work to be done the enough details are provided to allow any authorized and properly trained or competent person to carry out the work.	
The processes identify points for workers to certify that work has been done	
Verification of certification that work that is done was done is done.	
TOTAL (sum the ratings and divide by 8)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10

9.5.3 Control points and approval requirements

Rate each item from 0 to 10. Sum the ratings and divide by 6 for a total rating.

Item	*Rate*
Process control points are used when risks associated with work exceeds management-defined risk thresholds of the worker.	
The approval process identifies at least two individuals with adequate authority and knowledge to make a reasonable and prudent decision about the risk at each control point.	
The risk and options are identified to decision makers for each control point on each invocation.	

Item	Rate
Approvals require that the responsible approving parties read, understand, and select from the options and that they be adequately authenticated for the risks involved.	
There are override mechanisms for urgent decisions when inadequate decision-making power is available that implement fail safe modes and audit all actions taken.	
The effectiveness, operation, and validity of control points are tested and audited regularly.	
TOTAL (sum the ratings and divide by 6)	

Startup	Diligence	Typical	Excellent	Best
1.8	5	5	7	10

9.5.4 Appeals processes and escalations

Rate each item from 0 to 10. Sum the ratings and divide by 6 for a total rating.

Item	Rate
Work flows have suitable provisions for appeals and escalations when something that one person wants to have done is at odds with someone in the approval path.	
TOTAL (enter the rating)	

Startup	Diligence	Typical	Excellent	Best
0	1	1	1	1

9.5.5 Authentication requirements & mechanisms

Rate each item from 0 to 10. Sum the ratings and divide by 7 for a total rating.

Item	Rate
The quality and quantity of authentication associated with different functions is matched to the surety level required.	
Authentication for medium risk decisions require at least two factors.	
Authentication for high risk situations requires at least three factors.	
Multiple layers of authentication, when used, consider that reuse of the same authenticator only minimally increases surety in most cases.	
High risk decisions require physical presence of the decision-maker except in prespecified and top management approved cases.	
Multiple party authentication is required for high risk circumstances except in prespecified and top management approved cases..	
The work flow system supports the use of different authentication mechanisms to support the different levels of surety required to perform different operations.	

Item	Rate
TOTAL (sum the ratings and divide by 7)	

Startup	Diligence	Typical	Excellent	Best
1.8	5	5	7	10

9.5.6 Authorization and context limitations

Rate each item from 0 to 10. Sum the ratings and divide by 3 for a total rating.

Item	Rate
Authorizations associated with identified subjects under different levels of authentication change with context and situations within work flows.	
The work flow system is capable of handling complexities associated with the specific identified needs of data owners for access to the resources necessary to do work.	
The work flow system helps to prioritize work so that more important or time critical work is given proper priority.	
TOTAL (sum the ratings and divide by 3)	

Startup	Diligence	Typical	Excellent	Best
1.8	5	5	7	10

9.5.7 Work flow documentation and audit

Rate each item from 0 to 10. Sum the ratings and divide by 4 for a total rating.

Item	Rate
The work flow system provides documentation of what was done and what is to be done and allows this information to be read for audit purposes as appropriate.	
Detailing is available to the specific actions taken by specific individuals at specific times, the approvals required and obtained, and the work flow requirements of the situation at the time is documented so that all of the information needed to validate an action after the fact can be made available to the reviewer or auditor.	
Everything needed to determine what was done, why, when, how, where, and under what situational circumstances is available to check on any specific process undertaken or all of the processes of the system.	
Work flow documentation is hard enough to alter, forge, and destroy to meet the surety requirements of the work flow system.	
TOTAL (sum the ratings and divide by 4)	

Startup	Diligence	Typical	Excellent	Best
1.8	5	5	7	10

9.5.8 Control and validation of the engine(s)

Rate each item from 0 to 10. Sum the ratings and divide by 2 for a total rating.

Item	*Rate*
The work flow mechanisms that control security-related business processes are controlled, verified, validated, tested, reviewed, and tracked to assure that they do what they are supposed to do in practice.	
Verification and validation covers normal operation, all exception conditions and malicious attempts to circumvent the system at every level of its operation to the level of surety associated with the risks the work flow system helps to manage.	
TOTAL (sum the ratings and divide by 2)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10

9.5.9 Risk aggregation in the engine(s)

Rate each item from 0 to 10. Sum the ratings and divide by 5 for a total rating.

Item	*Rate*
Executive management and risk management explicitly address how much risk can be aggregated before additional protective measures are required.	
The risk acceptance thresholds are applied to work flow systems at every level they exist including but not limited to provisioning systems, HR systems, accounting systems, documentation systems, ticket management systems, identity management systems, pass3word reset and management systems, single sign on systems, and the infrastructures that support these systems.	
The cost savings associated with work flow is balanced against the risks presented by them for low surety situations.	
For medium and high risk systems, risk aggregation beyond the surety level of the work flow system is not permitted.	
As the work flow system reaches to risk levels where single individuals can no longer be permitted to make decisions, those systems are made multi-person control or other compensating controls are used.	
TOTAL (sum the ratings and divide by 5)	

Startup	*Diligence*	*Typical*	*Excellent*	*Best*
1.8	5	5	7	10