7.3.4 Personnel (human resources)

Human resources and legal issues are usually only indirectly under the control of the CISO function, and yet they are critically important to that function. These measures mix the ability to control process with the functional performance of the mechanisms.

Rate each issue from 0 to 10 in terms of current situation and goal. Then total the columns and divide rating by goal and multiply by 10 to generate a measure.

7.3.4.1 People life cycles

Issue	*Rate*	*Goal*
Use the life cycles rating here.		

7.3.4.2 Knowledge

Issue	*Rate*	*Goal*
Qualifications for specific jobs include security related degrees and certificates.		
Knowledge of the individuals act as prerequisites for certain tasks and jobs.		
Job history is a basis for security-related jobs.		
Defined areas of specialty for security are included in HR job descriptions.		
Educational benefits include provisions for computer security related education.		
Preference for information security positions are given based on degrees in related fields.		

7.3.4.3 Awareness

Issue	*Rate*	*Goal*
Awareness levels in defined areas are tracked.		
Certification for specific systems based on verified awareness are required for all workers.		
Workers not in compliance with awareness requirements are suspended from that work.		
Security awareness programs train and verify understanding for each worker every 6 months.		

Issue	*Rate*	*Goal*
Measurements of security awareness are used for evaluation of the HR function.		
The CISO function has great influence over the specifics of the security awareness program.		

7.3.4.4 Background

Issue	*Rate*	*Goal*
Background checks are done on all workers prior to hiring.		
All workers have criminal background checks.		
All workers have all references checked.		
All workers have job history verified.		
More in-depth checks are used for workers in more highly sensitive or trusted positions.		
Detailed clearance processes are used for select high consequence jobs.		
Workers are rechecked periodically.		

7.3.4.5 Trustworthiness

Issue	*Rate*	*Goal*
A systematic approach to evaluation of trust, including time in position and life-related characteristics is used.		
Trustworthiness is a key issue in employee evaluations.		

7.3.4.6 History

Issue	*Rate*	*Goal*
Security-related employee history is retained during employment.		
Security-related history includes all incidents involving the individual and detailed audit records attributed to the individual.		
Personnel records are examined for missing history at least yearly.		
Missing history in personnel records requires immediate remediation and investigation.		
History is provided to potential managers prior to transfer.		

7.3.4.7 Capabilities

Issue	*Rate*	*Goal*
Capabilities associated with individuals are tracked and used in evaluating suitability for positions and tasks.		
Information protection skills are specifically collected and used in assessing potential for positions in this area.		

7.3.4.8 Intents

Issue	*Rate*	*Goal*
Intents as expressed in written material are retained as part of the personnel record of individuals.		

7.3.4.9 Modus operandi

Issue	*Rate*	*Goal*
Personnel policy dictates the extent to which personal characteristics may be kept and used for different purposes.		
Personnel policy is enforced effectively.		
Workers are notified of any and all collection, dissemination, and use of this information		

7.3.4.10 Roles

Issue	*Rate*	*Goal*
Roles are associated with groups of individuals by the HR department as part of identity management.		
Rules on sets of roles for individuals over time are maintained and enforced by HR.		
Roles and rules for those roles assure that separation of duties requirements are met.		
Roles are granted based on qualifications and management request and approval.		
Roles are translated into authorizations and revocations associated with access devices including keys, accounts, and authenticators.		
Operational continuity is enforced by HR assuring that adequate qualified workers are in and trained for work in each identified role.		

7.3.4.11 Changes

Issue	*Rate*	*Goal*
Changes of employment status, job title, responsibilities, and roles are tracked by HR.		
Changes are instantiated so that information and system access is immediately changed to meet the new situation.		
Changes impacting access are verified as received and acted upon by HR.		
Revocation processes are particularly critical and HR tracks these to assure performance.		

7.3.4.12 Clearances

Issue	*Rate*	*Goal*
Every worker has at least one clearance associated with them.		
Clearances are associated only with individual human persons.		
Clearances are generated through defined and formal processes.		
Clearances are only granted after authorized approvals.		
Clearances are tracked and maintained by HR systems.		
Clearances reflect trust levels according to applicable standards.		
Clearances limit roles that may be associated with individuals.		
Clearances may be suspended by suspicion.		
Clearances may only be revoked for cause.		
A formal process for evaluating and reviewing clearances and appealing revocations is used.		

7.3.4.13 Need to know

Issue	*Rate*	*Goal*
Need-to-know (NTK) relates people to projects.		
NTK is tracked by HR as associated with roles.		
NTK is tracked to personnel records for history.		
HR data on NTK is confidential and protected against exploitation in entry, storage, use, and transit.		
NTK does not override clearances for access.		

7.3.4.14 IdM interface

Issue	*Rate*	*Goal*
HR uses IdM interfaces to input and track information on individuals.		
IdM tracks clearances, NTK, and histories.		
HR records track accurately to IdM in audits.		
IdM is protected to the highest level of any access it can be used to control.		
HR is authoritative with respect to IdM data.		

7.3.4.15 Roll-up

Area	*Issue*	*Rate*	*Goal*
TOTAL	Add up ratings and goals and enter the sums.		
Rating	Divide rating into goal and multiply by 10.		640

Based on total rating / 64

Startup	***Diligence***	***Typical***	***Excellent***	***Best***
1.5	4.5	6	8	9.5