PERFORMANCE EVALUATION ALL ISO STANDARDS

Management System has immense significance in business and other fields and huge amount of money is being spent on this around the globe to mitigate the risks. It is necessary to evaluate the outcome of information security system. In order to direct the process of management information in systems in the right direction, the activity of evaluation provides supervision. Evaluation is considered to be "undertaken as a matter of course in the attempt to gauge how well current organization meets a particular expectation & objective of compliance.

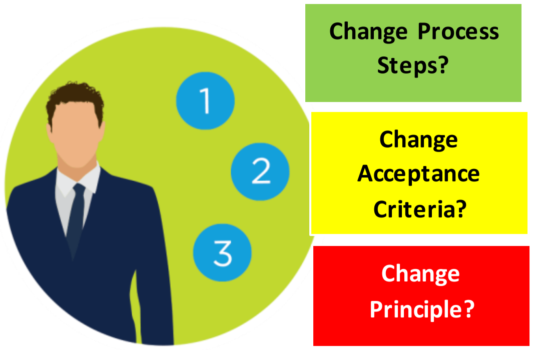
Evaluation of Management System Compliance Level

The consequence of such an assessment can then be used in the decisions of an organization when managing their management systems. Throughout the life cycle of an management system organization has to take important decisions. The most obvious of which are the go/no-go investment decisions.

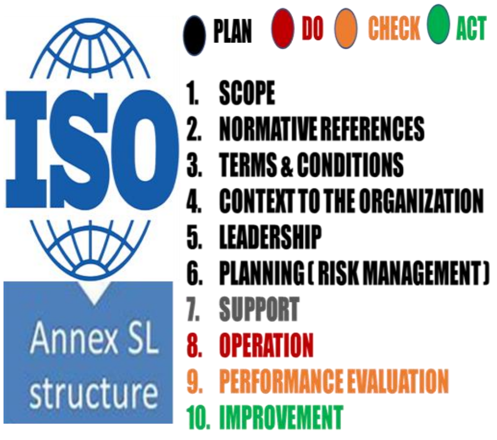
Change Management in Management Systems

Change management (sometimes abbreviated as CM) is a collective term for all approaches to prepare, support, and help individuals, teams, and organizations in making organizational change for improvements. Drivers of change in includes:

- **Reduction in Incidents**
- **Reduction in Non-Acceptable Residual Risks**
- **Reduction in Risks of Data Confidentiality & Data integrity**
- **Reduction in Risks for Human Confidentiality & Integrity**
- **Increase in Availability of required information**
- **Increase in Acceptable Residual Risks**
- **Increase in Risk Appetite**
- **Increase in Resilience**

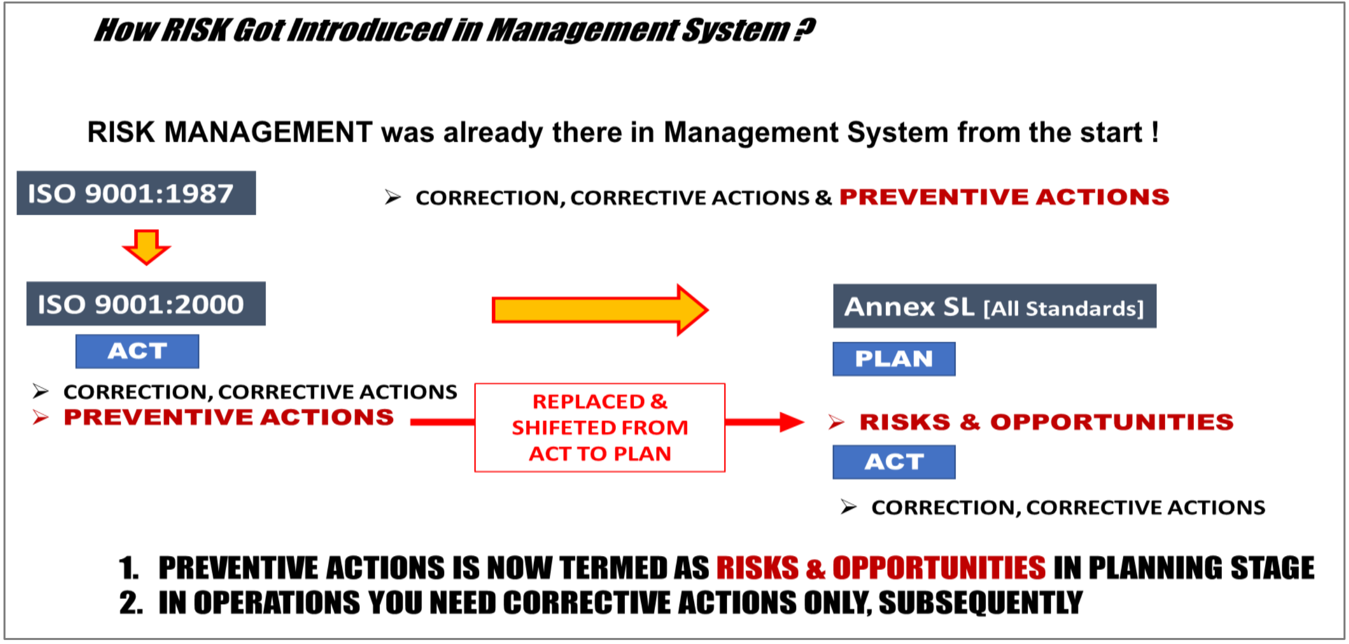


What is the ground reality in Management Systems?



In audits and trainings global experience, it has beer noticed that Performance & Evaluation is not done on holistic view to judge the effectiveness of Management Standards, including objectives set. There is still an understanding issue with setting objectives in Annex SL, on which all ISO Standards are currently based on, from 2012 onwards.

Annex SL is a section of the ISO/IEC Directives part 1 that prescribes how ISO Management System Standard standards should be written. The aim of Annex SL is to enhance the consistency and alignment of MSS by providing a unifying and agreed-upon high level structure, identical core text and common terms and core definitions. The aim being that all ISO Type A MSS are aligned and the compatibility of these standards is enhanced.



How RISK Got Introduced in Management System ?

RISK MANAGEMENT was already there in Management System from the start !

ISO 9001:1987

➢ CORRECTION, CORRECTIVE ACTIONS & PREVENTIVE ACTIONS

ISO 9001:2000

ACT

➢ CORRECTION, CORRECTIVE ACTIONS
➢ PREVENTIVE ACTIONS

REPLACED & SHIFETED FROM ACT TO PLAN

Annex SL [All Standards]

PLAN

➢ RISKS & OPPORTUNITIES

ACT

➢ CORRECTION, CORRECTIVE ACTIONS

1. PREVENTIVE ACTIONS IS NOW TERMED AS RISKS & OPPORTUNITIES IN PLANNING STAGE
2. IN OPERATIONS YOU NEED CORRECTIVE ACTIONS ONLY, SUBSEQUENTLY

IS PREVENTIVE ACTION = RISK ASSESSMENT?

Risk Assessment in Planning stage now, gives a better clarity to take all precautionary measures in advance, which is nothing Preventive Actions only.
Current Risk Assessment is the current System Baseline.
So in operations, when any Incident occurs, then only Corrections and Corrective Actions needed. No need to have any preventive action now. Hence you would find Preventive Action words in any of the standards, as it is replaced by Risk Assessment.

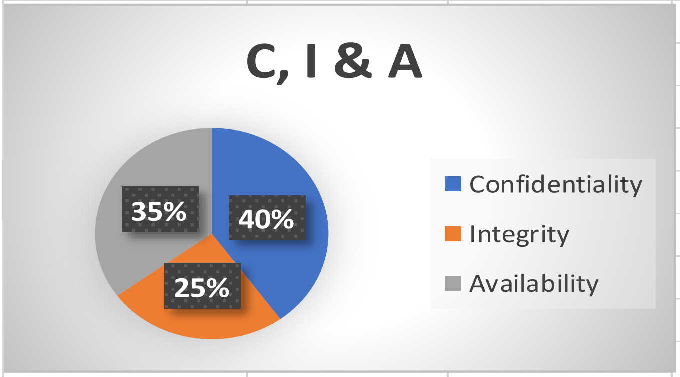
Concept of Setting OBJECTIVES?

Earlier the objectives for achievements were done in the beginning of compliance standard, when POLICY was designed. Now in ANNEX SL/L, first, the baseline understanding is done after RISK ASSESSMENT in planning stage, before setting OBJECTIVES, if you compare with climbing stairs, you lift one leg to put on next step, which you are confident of stability of other leg on the base & if you are not confident, you will not climb. So here also until you know the base line from Risk, one cannot set objectives.

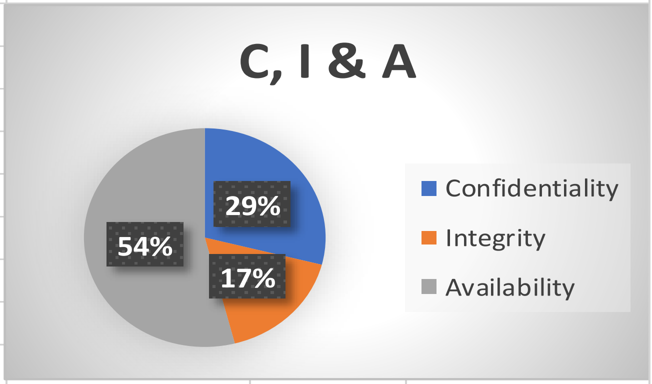
CLAUSE 6

Example (ISO 27001:2013):
If the status of C, I & A of two companies is as under:

COMPANY A		
OVERALL CONSUOLIDATION RISK ASSESSMENT OUTCOME		
Confidentiality	Integrity	Availability
40%	25%	35%
C & I > A		



COMPANY B		
OVERALL CONSUOLIDATION RISK ASSESSMENT OUTCOME		
Confidentiality	Integrity	Availability
29%	17%	54%
C & I < A		



There is not doubt that Company B is better than Company A, as C & I risks are less than A, which is acceptable as if A is not there, C & I are any way not there as access is not there on max. side. In Company A, C, I Risks are more than A, hence this company is in more danger than Company B.

Now the main question is setting good objectives for both?
Following are recommended (these are only broad examples):

Objective Setting for Company A

	Confidentiality	Integrity	Availability
Objective>	Reduce by 10% / Year	Reduce by 10% / Year	Reduce by 10% / Year
Who will do?	CISO + IT	CISO + IT + HOD	CISO + IT
What to do?	Better Mitigations in IT breaches	Better Mitigations in IT & Human Integrity breaches	Better Mitigations in IT breaches
Which Resources?	Incidents Information (KEDB) & Re-Risk Assessments (Regularly)	Incidents Information (KEDB) & Re-Risk Assessments (Regularly)	Incidents Information (KEDB) & Re-Risk Assessments (Regularly)
Competion Period?	Incident Information & Monitoring Results of Audits, Regulatory compliances etc.		
How to check Effectiveness	Regular monitoring of these objectives and corrective actions etc.		

Objective Setting for Company B

Confidentiality	Integrity	Availability	
Reduce by 10% / Year	Reduce by 10% / Year	Reduce by 10% / Year	Objective>
CISO + IT	CISO + IT + HOD	CISO + IT	Who will do?
Better Mitigations in IT breaches	Better Mitigations in IT & Human Integrity breaches	Better Mitigations in IT breaches	What to do?
Incidents Information (KEDB) & Re-Risk Assessments (Regularly)	Incidents Information (KEDB) & Re-Risk Assessments (Regularly)	Incidents Information (KEDB) & Re-Risk Assessments (Regularly)	Which Resources?
Incident Information & Monitoring Results of Audits, Regulatory compliances etc.			Competion Period?
Regular monitoring of these objectives and corrective actions etc.			How to check Effectiveness

Which areas can be monitored and Objectives set, which definitely improvements can be Effectively evidenced?

Following can be considered as KPI's (Key Performance Indicators for any Management System:

- **Reduction in Incidents with KEDB (Known Error Data Base)**
- **Reduction in Non-Acceptable Residual Risks**
- **Reduction in Risks of Data Confidentiality & Data Integrity**
- **Reduction in Risks for Human Confidentiality & Integrity**
- **Increase in Availability of required information**
- **Increase in Acceptable Residual Risks**
- **Increase in Risk Appetite**
- **Increase in Resilience**
- **Increase in Compliance (Information of Internal Audits, Regulatory & Governance Commitments**
- **Increase in Process, Acceptance Criteria etc. Awareness for total population.**