Proposed Risk Culture Framework for Commercial Air Transport Organisations

Sir Charles Haddon-Cave's 'Four State of Man' →			Risk Ignorant	Risk Cavalier	Risk Averse	Risk Sensible
Understanding Risk vs Risk Exposure →→			**Understanding of risk is LOW Risk Exposure is also HIGH**	**Understanding of risk is HIGH Risk Exposure is HIGH**	**Understanding of risk is LOW Risk Exposure is LOW but Excessive which is costly**	**Understanding of risk is HIGH Risk Exposure is LOW and ALARP**
IRM Risk Culture Aspects Model	**RISK MANAGEMENT PROCESSES (Based on ICAO SMM & ISO 31000)**	**Risk Identification (ISO 31000 - Recording & Reporting and Risk Communication bottom up)**	Identification of Risk is based on reactive processes such as accidents / serious incident investigations.	Identification of Risk is based on reactive processes such as accident/occurrence investigation and there may be some other means of reporting hazards and risks	Risk/Hazard Identification is based on both reactive (accident/incident investigations) and proactive methods (voluntary hazard/risk reporting)	Risk/Hazard Identification is based on both reactive (accident/incident investigations) and proactive methods (voluntary hazard/risk reporting) The organisation also continually uses external data sources to identify risks and takes part in collaborative efforts in the industry.
		Risk Analysis (ISO 31000 - Scope, Context, Criteria)	There is no risk analysis process to consider the context, worst credible scenario etc.	Superficial level of risk analysis is carried out without fully understanding the context and taking that into account.	Very limited analysis of risks take place and results in poor understanding of risks the organisation faces.	Risks are analysed in depth and articulated based on contextual information. The analysis enables the organisation to understand all the credible outcomes and their probability for occurrence.
		Risk Assessment (ISO 31000 - Consultation)	Risks are assessed based on a risk matrix adopted from a source without any consultation with all stakeholders including front line operators. Risk assessment activity is seen as a 'tick in the box' exercise rather than key decision making process to allocate resources efficiently and effectively.	Risks are assessed based on a risk matrix adopted from a source without any consultation with all stakeholders including front line operators.	Risk assessments consider worst case scenarios that are not credible and the probabilities are overestimated due to lack of consultation with all stakeholders including frontline operators.	Risk are assessed based on the analysis carried out with the involvement of all stakeholders including frontline operators.
		Risk Control (Elimination or Mitigation) (ISO 31000 - Treatment & Communication)	Risk controls are only put in place to react to accidents and serious incidents. They are not well thought mitigation actions and they do not reduce the exposure to risks. The decisions to stop / not conduct operations are never considered.	Risk controls are not well thought mitigation actions and reduce safety margins. The decisions to stop / not conduct operations are very rarely considered.	Risk Controls are developed to cover extremely improbable scenarios or the worst case scenarios are not credible. Risk mitigation measures cost the organisation unnecessary financial burden without reducing exposure to risk.	Risk Controls are well thought mitigation actions to achieve ALARP but risks are eliminated - when necessary - by stopping / not conducting operations.
		Risk Monitoring & Review	Risk controls are not monitored during audits and inspections and not reviewed by the management on a regular basis.	Risk controls are monitored during audits and inspections but the effectiveness of mitigation actions are not carefully evaluated even though the regular reviews by the management take place.	The risk controls are monitored and regularly reviewed but the analysis and assessment decisions are not challenged to find a balanced approach. For example, cost benefit analysis is not considered as safety is seen as number one priority.	The risk controls are monitored and regularly reviewed to continually reanalyse and reassess risks based on the changing environments the organisation operates. When necessary, cost benefit analysis is carried out.
	Tone at the top	**risk leadership - clarity of direction**	There is no clarity from the top management about risk tolerability e.g. risk appetite, acceptable vs unacceptable risks	There is no clarity from the top management about risk tolerability e.g. risk appetite, acceptable vs unacceptable risks. Leadership communicates their position only when events happen	Top management's position on risk tolerability is very clear but also very cautious. There is no appetite for any risk taking regardless of the cost implications.	Top management's position on risk tolerability is very clear and enables the organisation to make balanced decisions based on . There is no appetite for any risk taking regardless of the cost implications.
		how the organisation responds to bad news	The organisation responds to bad news very poorly and starts blaming individuals for not managing risks effectively. There is no learning opportunity to improve risk management processes	The organisation accepts the bad outcomes as unpredictable events and does not seek to understand the context or causal factors in depth. As a result, there is no learning opportunity to improve processes impacting on risk decision making and/or changing behaviours.	The organisation responds to bad news immediately by taking extreme measures to react towards an even more risk averse position.	Bad outcomes are immediately evaluated and any reactive measures are carefully considered but not put in place unless they are absolutely necessary.
	Governance	**the clarity of accountability for managing risk (Risk Ownership)**	Risk ownership is not defined at all despite there are clear responsibilities defined in terms of safety etc.	There is some level of clarity in terms of risk ownership but in practice the accountabilities for managing risks are not well understood and agreed.	The accountabilities for managing risks are well defined including when risk decisions should be escalated to top management so that frontline operators and line managers cannot take any risks	The accountabilities for managing risks in various operational areas are well defined and understood by all frontline operators and managers. While certain operational risk decisions are made by frontline operators and their line managers, they also understand when certain risk decisions need to be escalated to top management level.
		the transparency and timeliness of risk information (Risk Communication - top down)	There may or may not be a risk register but it is only updated based on accidents and serious incidents. This is not always reviewed by the top management and it is not communicated to all stakeholders including the frontline operators.	There is a risk register and it updated based on bot reactive and proactive information sources however such risk information is not regularly reviewed by the top management as it is seen as the Safety Department's responsibility.	The risk register is kept up to date based on all the available information and any newly identified risks. The risk information is communicated across the whole organisation to prevent any individual making risk tolerant decisions.	Risk information (including risk register, risk analysis and assessment results and the key risk decisions) are completely available to all employees unless they are commercially sensitive or security restricted. Organisation uses all information sources to identify new risks and react to the assessment in a timely manner.
	Competency	**the status, resources and empowerment of the risk function**	Risk Management is not visible in organisation's daily activities. Sufficient resources are not provided for intolerable risk mitigations in a timely manner. Who makes key risk decisions in the organisation is not defined and frontline operators are not allowed to make any risk decisions.	Although risk management is visible in organisation's daily activities, it is not valued or seen as crucial for making key decisions. Sufficient resources are not provided for intolerable risk mitigations in a timely manner. Who makes key risk decisions in the organisation is not defined and frontline operators are not allowed to make any risk decisions.	Risk management is visible in organisation's daily activities, it is used for making key risk decisions but always over protecting the organisation and individuals. Sufficient resources are provided for intolerable risk mitigations immediately or the operations stop. Key risk decisions in the organisation are always made with top management's involvement and not involve frontline operators. Or sometimes the frontline operators make very risk averse decisions regardless of the flexibility they are given e.g.. to be able to use discretion.	Risk Management is seen as an integral part of the business decision making process. It is valued at all levels in the organisation. Resources are provided for risk mitigation measures on the basis of well thought risk analysis and assessment involving all stakeholders. Well trained and competent frontline operators and their line managers are empowered to make certain risk decisions collaboratively however when they believe it is necessary, certain key risk decisions are escalated in the management chain (up to the SRB / AM level)
		risk skills - the embedding of risk management skills across the organisation	SMS Training may or may not cover some elements of risk management and risk based decision making but that is usually limited to management staff.	Although frontline supervisors and their line managers are or may be trained about the basic concepts of risk management and risk based decision making, their attitude is always leaning towards a more risk tolerant position due to internal and sometimes external factors.	Although frontline supervisors and their line managers are trained about the basic concepts of risk management and risk based decision making, their attitude is always leaning towards a more risk averse position due to internal and sometimes external factors	All staff from Accountable Manager to frontline supervisors and their line managers are well trained based their accountabilities as well as their authorities. Each employee fully understands the basic concepts of risk management and risk based decision making and most importantly when to escalate certain key risk decisions.
	Decision making	**well informed risk decisions**	Risk decisions are made by either gut feelings or based on ill-informed processes	Risk decisions are not always based on sound risk analysis despite the fact that reasonably good risk information is available. As a result risk decisions are made and create unnecessary exposure.	Risk decisions are not based on sound risk analysis despite the fact that reasonably good risk information is available. As a result, very costly risk decisions are made due to lack of understanding the risk.	All risk decisions are made collaboratively involving all stakeholders and they are based on sound risk analysis and assessment.
		appropriate risk taking rewarded and performance management linked to risk taking.	The organisations has no clear policy, procedure and any training for employees and managers about risk taking behaviour.	Risk taking is seen as part of operational decision making and sometimes unnecessary risk taking is also tolerated by the management as long as the outcome is positive for the organisation	Risk taking is not tolerated at all. It is clearly communicated from the top management as a punishable behaviour.	Risk taking (Tolerating certain risks) based on well thought and sound risk analysis and assessment is tolerated even though it is not encouraged. This is seen as part of organisation's overall risk management strategy.

NOTE: Please note that various terms used above such as risk taking, risk tolerance etc. do not necessarily mean that the organisation or individuals choose to NOT COMPLY with the regulations or not. In operational environment, everyday, many frontline operators and their line managers have to make judgements based on the information available to them at the time. This also means they sometimes have to make operational decisions tolerating a certain level of risk without being non-compliant with the safety regulations or company procedures. Same also applies to senior and top management as well. So the risk culture terminology should not always be interpreted as risk taking means non-compliance.