

# KEY LESSONS FROM THE COLUMBIA SHUTTLE DISASTER

*(WITH ADAPTATION TO THE PROCESS INDUSTRIES)<sup>1</sup>*

## *An “Organizational Culture” Question Set for Improving Operational Excellence in HSE Management*

**“In our view, the NASA organizational culture had as much to do with this accident as the foam.”**

*CAIB Report, Vol. 1, p. 97*

### *I. Overview*

On February 1, 2003, the Space Shuttle Columbia disintegrated during re-entry into the Earth’s atmosphere, killing all seven crewmembers aboard. The direct chain of events leading to the disaster had begun 16 days earlier when the Shuttle was launched. During ascent, 81 seconds after liftoff, a large chunk of insulating foam broke off of the external fuel tank, struck the Shuttle, and damaged critical thermal protection tiles. The tiles subsequently failed when exposed to the intense heat encountered when the shuttle re-entered the atmosphere during its return to Earth.

While the foam strike was discovered during the review of launch videos on the second day of the mission, Shuttle Program management could not be convinced that the event posed a hazard to the mission, the spacecraft, or the crew. Consequently, there was no formal effort put forward to confirm the integrity of the Columbia shuttle before its ill-fated return to Earth.

Following the tragedy, the *Columbia Accident Investigation Board* (CAIB) was formed. After determining that insulating foam debris striking the wing was the most likely physical cause, the Board turned its attention to the organizational culture factors behind the failure. For the purpose of its investigation, the Board offered the following definition of organizational culture:

**“Organizational culture refers to the basic values, norms, beliefs, and practices that characterize the functioning of a particular institution. At the most basic level, organizational culture defines the assumptions that employees make as they carry out their work; it defines “the way we do things here.” An organization’s culture is a powerful force that persists through reorganizations and the departure of key personnel.”**

*CAIB Report, Vol. 1, p. 101*

---

<sup>1</sup> Developed by David Jones (Chevron), Walt Frank (ABS Consulting), Karen Tancredi (DuPont), and Mike Broadribb (BP).

In pursuing the investigation beyond immediate causal contributors, the CAIB was trying to understand two issues in particular:

- Why was it that serious concerns about the integrity of Columbia, raised within one day of launch, were not acted upon in the two weeks available between launch and return? With little corroborating evidence, management had become convinced that a foam strike was not, and could not be, a concern.
- Which of the cultural patterns emerging from the Columbia accident were the same as those first identified after the Challenger tragedy (almost exactly 17 years earlier) and why were they still present?

Through its report, the CAIB has provided a service to all organizations that operate facilities handling hazardous materials or that engage in hazardous activities. Although NASA is a unique organization, with a focused mission, the organizational cultural failures that led to the Columbia disaster have counterparts in any operation with a potential for significant incidents. Key organizational cultural themes emerging from the CAIB report include:

- 1. Maintaining a Sense of Vulnerability** Catastrophic incidents involving highly hazardous materials or activities occur so infrequently that most organizations never have the unfortunate, but educating, opportunity of experiencing one. Operating diligence and management effectiveness can be easily dulled by a sense of false security – leading to lapses in critical prevention systems. Eliminating serious incidents requires constant reminders of the vulnerabilities inherent in hazardous activities.
- 2. Combating Normalization of Deviance** When pre-established engineering or operational constraints are consciously violated, with no resulting negative consequences, an organizational mindset is encouraged that more easily sanctions future violations. This can occur despite well-established technical evidence, or knowledge of operational history, that suggests such violations are more likely to lead to a serious incident.
- 3. Establishing an Imperative for Safety** An organization that is focused on achieving its major goals can develop homogeneity of thought that often discourages critical input. In the case where valid safety concerns are ignored, the success of the enterprise can be put in jeopardy. The CAIB report makes a compelling argument for ensuring strong, *independent* “sanity” checks on the fundamental safety integrity of an operation.
- 4. Performing Valid/Timely Hazard/Risk Assessments** Without a complete understanding of risks, and the options available to mitigate them, management is hampered in making effective decisions. Organizations that do not actively engage in qualitative and quantitative “*what can go wrong?*” exercises, or that fail to act on recommendations generated by the risk assessments that are done, miss the opportunity to identify and manage their risks.
- 5. Ensuring Open and Frank Communications** A dysfunctional organizational culture can discourage honest communications, despite formal appearances to the contrary. This

is done through established protocol, procedures, and norms that dictate the manner in which subordinates communicate with management, and the manner in which management receives and responds to the information. Barriers to lateral communications (e.g., between work groups) can also impede the free flow of safety-critical information.

- 6. Learning and Advancing the Culture** Organizations that do not internalize and apply the lessons gained from their mistakes relegate themselves to static, or even declining, levels of performance. Safety excellence requires the curiosity and determination necessary to be a learning, advancing culture.

Brief summaries of the above themes, taken from the Columbia report, are offered below. In addition, “question-sets for self-examination” are included as initial, high level guidance should facilities wish, as part of their Operational Excellence integration efforts, to begin identifying and correcting organizational cultural parallels, if any, that may exist between NASA and their own operations.

## *II. Maintaining a Sense of Vulnerability*

**“Let me assure you that, as of yesterday afternoon, the Shuttle was in excellent shape, mission objectives were being performed, and that there were no major debris system problems identified...” Spoken by NASA official, following Columbia launch, and after a significant debris strike had been identified.**

*CAIB Report, Vol. 1, p. 101*

**“The Shuttle has become a mature and reliable system ... about as safe as today’s technology will provide.” Advisory Panel “Kraft Report,” March 1995**

*CAIB Report, Vol. 1, p. 108*

In the 17 years since the Challenger incident, the perception that similar catastrophic events could occur had been diminished by the NASA organizational culture. Shuttle managers were relying heavily on recent past success as a justification for their actions. Specifically, new, unforeseen issues were not subject to thorough technical analysis. For example, the belief that foam strikes did not jeopardize the Shuttle arose from a limited observation that no disasters had resulted from previous foam impacts -- so therefore, no disasters were going to occur in the future. Past success, and incident-free operation do not guarantee future success. Only a continuous focus on the fundamentals of safety management will keep risks to a minimum.

### **Maintaining a Sense of Vulnerability – Question-Sets for Self-Examination**

1. Could a serious incident occur today at one of our facilities, given the effectiveness of our current operating practices? When was the last serious close call or near miss? Do we believe that process safety management (PSM) or other compliance activities are guaranteed to prevent major incidents?

2. Are lessons from related industry disasters routinely discussed at all levels in the organization, with action taken where similar deficiencies have been identified in our operations?
3. Do risk analyses include an evaluation of credible major events? Are the frequencies of such events always determined to be “unlikely?” Have proposed safety improvements been rejected as “not necessary” because “nothing like this has ever happened?” Do risk analyses eliminate proposed safeguards under the banner of “double jeopardy?”<sup>2</sup>
4. Are critical alarms treated as operating indicators, or as near miss events when they are activated? Do we believe that existing safety systems will prevent all incidents?
5. Is the importance of preventive maintenance for safety critical equipment recognized, or is such work allowed to backlog? Are the consequences of failure of such equipment recognized and understood by all?
6. Are there situations where the benefits of taking a risk are perceived to outweigh the potential negative consequences? Are there times when procedures are deviated from in the belief that major outcomes will not be caused? What are these? Are risk takers tacitly rewarded for “successful” risk taking?

### ***III. Combating Normalization of Deviance***

“...Space Shuttle System, including the ground systems, shall be designed to preclude the shedding of ice and/or other debris from the Shuttle elements during pre launch and flight operations that would jeopardize the flight crew, vehicle, mission success, or would adversely impact turnaround operations.”

“...No debris shall emanate from the critical zone of the External Tank on the launch pad or during ascent except for such material which may result from normal thermal protection system recession due to ascent heating.”

**Ground System Specification Book – Shuttle Design Requirements**

*CAIB Report, Vol. 1, p. 122*

“Debris impact on port wing edge-appears to have originated at the External Tank forward bipod – foam? - if so, it shouldn’t be a problem” **Taken From Shuttle Managers Handover Notes on January 17, 2003**

*CAIB Report, Vol. 1, p. 142*

Ham: “It would be a turnaround issue only?”

McCormack: “Right.”

**Minutes From Columbia Shuttle Management Meeting, January 24, 2003**

*CAIB Report, Vol. 1, p. 161*

---

<sup>2</sup> “Double jeopardy” refers to a mindset, too common to process hazard analysis teams, that scenarios requiring two independent errors or failures need not be considered since they are “so unlikely to occur.”

Having lost the sense of vulnerability, the organization succumbed to accepting events that were precluded in the original shuttle design basis. Over the 113 Shuttle missions flown, foam shedding and debris impacts had come to be accepted as routine and maintenance concerns only. Limited or no additional technical analyses were performed to determine the actual risks associated with this fundamental deviation from intended design. Each successful landing reinforced the organization's belief to the point where foam shedding was "normalized." As new evidence emerged suggesting that the Columbia foam strike was larger, and possibly more threatening, than earlier foam strikes, this information was quickly discounted by management. The "understanding" that foam strikes were insignificant was so ingrained in the organizational culture that even after the incident, the Space Shuttle Program Manager rejected the foam as a probable cause, stating that Shuttle managers were comfortable with their "previous risk assessments."

It is significant that a similar "normalization of deviance" had played such a key role in the Challenger disaster seventeen years earlier. While the concept of "normalization of deviance" had been much discussed in the aftermath of the Challenger incident, the NASA culture had not been "cured" of this crucial weakness.

### **Combating Normalization of Deviance – Question-Sets for Self-Examination**

1. Are there systems in operation where the documented engineering or operating design bases are knowingly exceeded, either episodically, or on a "routine" basis? Examples might include flare systems with inputs added beyond the design capacity, process piping or equipment operating at or above the design limits, or systems operated in a significantly different manner than initially intended.
2. Have the systems meeting the above criteria been subjected to thorough risk assessments? Did issues of concern emerge from the risk assessments? Were they addressed appropriately?
3. Have there been operating situations in the past where problems were solved by not following established procedures, or by exceeding design conditions? Does the organizational culture encourage or discourage "creative" solutions to operating problems that involve circumventing procedures?
4. Is it clear who is responsible for authorizing waivers from established procedures, policies, or design standards? Are the lines of authority for deviating from procedures clearly defined? Is there a formalized procedure for authorizing such deviations?
5. What action is taken, and at what level, when a willful, conscious, violation of an established procedure occurs? Is there a system to monitor deviations from procedures where safety is concerned? Can staff be counted on to strictly follow procedures when supervision is not around to monitor compliance?
6. Do we have management systems that are sufficiently discerning and robust to detect patterns of abnormal conditions or practices before they can become accepted as the norm?

7. Are we knowingly accepting practices or conditions that we would have deemed unacceptable 12 months ago? ... 24 months ago?

#### ***IV. Establishing an Imperative for Safety***

“When I ask for the budget to be cut, I’m told it’s going to impact safety on the Space Shuttle ... I think that’s a bunch of crap.” **Daniel S. Goldin, NASA Administrator 1994**

*CAIB Report, Vol. 1, p. 106*

“...safety personnel were present but passive and did not serve as a channel for the voicing of concerns or dissenting views. Safety representatives ... were merely party to the analysis process and conclusions instead of an independent source of questions and challenges. Safety contractors... were only marginally aware of the debris strike analysis. One contractor did question the Debris Assessment Team safety representative about the analysis and was told that it was adequate. No additional inquiries were made. The highest-ranking safety representative at NASA headquarters deferred to Program managers when asked for an opinion on imaging of Columbia. The safety manager he spoke to also failed to follow up.”

*CAIB Report, Vol. 1, p. 170*

Whether or not the budget cuts to which Mr. Goldin was referring in the above quote would have actually impacted safety is irrelevant. The impact of such a statement on an organizational culture is significant -- especially when coming from a top official. People at all levels feel less compelled to bring up safety matters if they feel that top management is not interested. Others, at lower levels, begin to mimic the attitudes and opinions that they hear from above.

Over the years at NASA, the safety organization had degraded, and had ultimately been relegated to “rubber stamping” critical safety-related decisions, rather than providing an independent assessment, and strong voice, that would help ensure the management of risks. Most importantly, when safety staff expressed a concern about the safety of an operation, they were often put in the untenable position of having to prove that the operation was unsafe. This reversed the more traditional burden of proof, where engineers and managers are required to defend the safety of the operation.

During the Columbia flight this functional reversal (proving the incident will happen as opposed to proving it will not) extended to the engineering organization, which had concerns about the amount of damage caused by the foam impact. Imaging capabilities existed within the US government that could have provided photographic evidence of whether the shuttle wing had been damaged. Engineers were prohibited from obtaining such critical corroborating evidence of the actual damage because they could not prove that the damage existed... and they could not prove that the damage existed because they could not obtain the photographic evidence.

### **Establishing An Imperative For Safety – Question-Sets for Self-Examination**

1. Is there a system in place that ensures an independent review of major safety-related decisions? Are reporting relationships such that impartial opinions can be rendered? Is there a “shoot the messenger” mentality with respect to dissenting views?
2. Who are the people independently monitoring important safety-related decisions? Are they technically qualified to make judgments on complex process system designs and operations? Are they able to credibly defend their judgments in the face of knowledgeable questioning? Do safety personnel find it intimidating to contradict the manager’s/leader’s strategy?
3. Has the role of safety been relegated to approving major decisions as *fait accompli*? Do production and protection compete on an equal footing when differences of opinion occur as to the safety of operations?
4. Has the staffing of key catastrophic incident prevention positions (process safety management) been shifted, over the years, from senior levels to positions further down the organization? Are there key positions currently vacant?
5. Does management encourage the development of safety and risk assessments? Are recommendations for safety improvements welcomed? Are costly recommendations, or those impacting schedule, seen as “career threatening” – if the person making the recommendations chooses to persistently advocate them?
6. Is auditing regarded as a negative or punitive enterprise? Are audits conducted by technically competent people? How frequently do audits return only a few minor findings? Is it generally anticipated that there will be “pushback” during the audit closeout meetings?

### ***V. Performing Valid/ Timely Hazard/Risk Assessments***

“A fundamental element of system safety is managing and controlling hazards. NASA’s only guidance on hazard analysis is outlined in the Methodology for Conduct of Space Shuttle Program Hazard Analysis, which merely lists tools available. Therefore, it is not surprising that hazard analysis processes are applied inconsistently across systems, subsystems, assemblies, and components.”

*CAIB Report, Vol. 1, p. 188*

“Any more activity today on the tile damage or are people just relegated to crossing their fingers and hoping for the best?”

“I have not heard anything new. I’ll let you know if I do.”

**Email Exchange Between Engineers, January 28, 2002**

*CAIB Report, Vol. 1, p. 165*

The CAIB concluded that a lack of consistent, structured approaches for identifying hazards and assessing risks contributed to the faulty decision-making process at NASA. Many of the analyses that were performed contained subjective and qualitative judgments, using words like “believed” and “based on experience from previous flights this hazard is an *Accepted Risk*.” Further, many of the action items emerging from these studies were not addressed. As an example, 1000 infrastructure items identified in 2000 as “deplorable” and requiring attention were never fixed, due to a lack of funding.

Audits had repeatedly identified deficiencies in NASA’s problem and waiver tracking systems. Prior safety studies had identified 5396 hazards that could impact mission integrity. Of these, 4222 were ranked as “Criticality 1/1R,” meaning that they posed the potential for loss of crew and orbiter. However, associated safety requirements had been waived for 3233 of these 1/1R hazards and, at the time of the Columbia investigation, more than 36% of those waivers had not been reviewed in the previous 10 year period.

The failure of the risk assessment process is ultimately manifested in the Columbia incident. By the time the Shuttle had launched, there was still no clear technical, risk-based understanding of foam debris impacts to the spacecraft. The management had no solid information upon which to base their decisions. In lieu of proper risk assessments, most of identified concerns were simply labeled as “acceptable.”

### Performing Valid/Timely Hazard/Risk Assessments – Question-Sets for Self-Examination

1. Are risk assessments performed consistently for engineering or operating changes that potentially introduce additional risks? Who decides if a risk assessment should be performed? What is the basis for not performing a risk assessment?
2. How are risks for low frequency – high consequence events judged? Is there a strong reliance on the observation that serious incidents have not occurred previously, so they are unlikely to occur in the future? What is the basis for deeming risks acceptable – particularly those associated with high consequence events?
3. Are the appropriate resources applied to the risk assessment process? Are senior level personnel, with appropriate technical expertise, enlisted for the risk assessment? Are the recommendations emerging from the risk assessments meaningful?
4. What are the bases for rejecting risk assessment recommendations?
  - Subjective judgment, based upon previous experience and observation?
  - Objective assessment, based upon technical analysis?
5. Are the risk assessment tools appropriate for the risks being assessed? Are qualitative or quantitative tools used to assess risks associated with low frequency – high consequence events? Are the tools deemed appropriate by recognized risk assessment professionals?

6. Do we have a system, with effective accountabilities, for ensuring that recommendations from risk assessments are implemented in a timely fashion, and that the actions taken achieve the intent of the original recommendation?

## ***VI. Ensuring Open and Frank Communications***

“In my humble technical opinion, this is the wrong (and bordering on irresponsible) answer ... not to request additional imaging help from any outside source. I must emphasize (again) that severe enough damage ... combined with the heating and resulting damage to the underlying structure at the most critical location ... could present potentially grave hazards. The engineering team will admit it might not achieve definitive high confidence answers without additional images, but, without action to request help to clarify the damage visually, we will guarantee it will not ... Remember the NASA safety posters everywhere around stating, “If it’s not safe, say so?” Yes, it’s that serious.” **Memo to File – Shuttle Engineer, January 22, 2003**

*CAIB Report, Vol. 1, p. 157*

The above memo was never sent. It expresses concern over the fact that NASA management had denied a request to obtain satellite photo images of the Shuttle wing damage. The imaging would likely have shown that potentially catastrophic damage had occurred. The CAIB’s report suggests a number of reasons why the true technical concerns of the engineers were never seriously considered and why accurate and truthful concerns, such as those expressed in the above memo, never left the filing system.

- The management had already settled on a uniform mindset that foam strikes were not a concern. Any communications to the contrary were either directly or subtly discouraged.
- An organizational culture had been established that did not encourage “bad news.” This was coupled with a NASA’s culture that emphasized “chain of command” communications. The overall effect was to either stifle communications completely, or, when important issues were communicated, to soften the content and message as the reports and presentations were elevated through the management chain.
- Engineering analysis was continually required to “prove the system is unsafe” rather than “prove the system is safe” – without any hard data available to support either position.
- The organizational culture encouraged 100% consensus. (The CAIB observed that a healthy safety organization is suspicious if there are no dissenting views). In this environment, general dissention was tacitly discouraged. Participants felt intimidated.

Despite these obstacles, and without encouragement (indeed, in the face of direct discouragement) engineers continued to work nights and weekends to gain a technical understanding of the foam damage. The organizational culture never allowed the strong, heartfelt, and accurate concerns of engineering personnel to surface in the management decision-making process.

### Ensuring Open and Frank Communications – Question-Sets for Self-Examination

1. How does management encourage communications that contradict pre-determined thoughts or direction? How are contradictory communications discouraged? Is the bearer of “bad news” viewed as a hero, or “not a team player?”
2. Does the organizational culture require “chain of command” communications? Or is there a formalized process for communicating serious concerns directly to higher management? Is critical, safety-related news that circumvents official channels welcomed?
3. Do communications get altered, with the message softened, as they move up the management chain? Why does this happen? Is there a “bad news filter” along the communications chain?
4. Do management messages on the importance of safety get altered as they move down the management chain? Do management ideals get reinterpreted in the context of day-to-day production and schedule realities?
5. Are those bearing negative safety-related news required to “prove it is unsafe?”
6. Has the “intimidation” factor in communications been eliminated? Can anyone speak freely, to anyone else, about their honest safety concerns, without fear of career reprisals?
7. Does the culture prompt a “can do” or “we cannot fail” attitude that overrides a common-sense awareness of what is truly achievable, and stifles opinions to the contrary?

### *VII. Learning and Advancing the Culture*

“... the Board strongly believes that if these persistent, systemic flaws are not resolved, the scene is set for another accident.” CAIB commenting on their conclusion that the organizational deficiencies that caused Challenger had remained to cause Columbia.

*CAIB Report, Vol. 1, p. 195*

The parallels between the organizational culture deficiencies contributing to the Challenger incident and those contributing to the Columbia incident were frequent and compelling. For example:

- The integrity and potency of the safety oversight function had been allowed to again erode.
- An overly ambitious launch schedule (relative to the capabilities of the organization) was again imposing an undue influence on safety-related decision-making.
- NASA was once again relying on “past performance as a guarantee of future success.”

- Conditions and events totally inconsistent with NASA's technical basis for mission safety were still being "normalized."
- Rigid organizational and hierarchical policies were still preventing the free and effective communication of safety concerns. Rank and stature were once again trumping expertise.

NASA had not effectively drawn learnings from the Challenger incident, and its safety culture had not sufficiently advanced in the intervening 17 years. Implementing cultural change can be slow, hard work. It begins by leaders consistently modeling and reinforcing the attitudes and behaviors expected in the new culture. Results would suggest that this had not happened at NASA.

### **Learning and Advancing the Culture – Question-Sets for Self-Examination**

1. Are corporate and site leaders aware of the essential features of a sound safety culture? Do they understand their personal responsibilities for fostering and sustaining the safety culture? Are they meeting these responsibilities?
2. Do leaders consistently model and support the attitudes and behaviors we expect of our culture? Do the workers?
3. Are we monitoring our operations closely enough to detect problems? How do we ensure the objectivity necessary to see those problems for what they are?
4. Do we have systems for reliably learning from our mistakes? Do we willingly and enthusiastically accept those learnings and apply them to improve our systems and procedures?
5. Where are we now vs where we hope to be with respect to our safety culture? Where do we want to be a year from now? ... two years from now? How do we plan to get here?
6. If we are comfortable with where we are now, how do we discriminate between comfort and complacency?

## ***VII. Intention and Limitations of the Question-Sets***

The above question-sets summarize lessons from the Columbia incident only, and should not be automatically applied - as is - to other organizations. NASA's experience may or may not be wholly or directly applicable to the unique features of each organizational culture. The question sets are intended to serve only as a starting point in determining the relevancy of the Columbia experience. More importantly, by opening a dialog on this important issue, organizations may be able to further enhance ongoing cultural improvement efforts.

If the process proves valuable, it is anticipated that additional question-sets would be generated, as a means to facilitate different workgroups within the Company in exploring their own organizational cultural weaknesses.