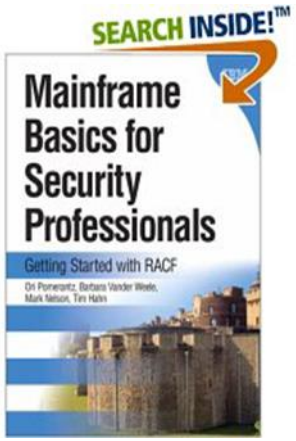
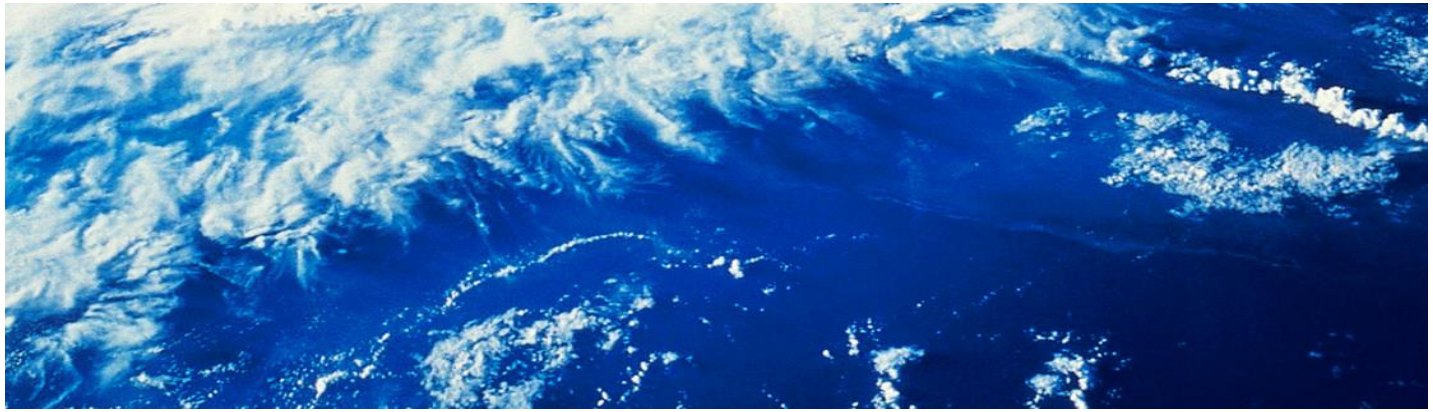
High Expectations: Our Systems are (*or could be*) like Airplanes

New York RACF Users Group

Mark Nelson, CISSP®, CSSLP®
RACF Design and Development
IBM Poughkeepsie
markan@us.ibm.com

David Hayes
Auditor
U.S. Government Accountability Office
hayesd@gao.gov





Comparing Aviation and Information Technology – Similarities and Differences

Comparisons of Aviation and Information Technology

- **Roots of the modern industry**
  - 1904: Wright Brothers first flight heavy-than-air powered flight
  - 1884: Hollerith files his patent application titled "Art of Compiling Statistics”
- **Coming of age**
  - 1939: Introduction of the DC3 (the first airliner capable of non-stop long distance flights) and the growth of airlines
  - 1940s: Stored programmable systems – the move away from mechanical computation of data
- **Innovation spurs expansion**
  - 1960s: Boeing 707 and 747
  - 1960s: System/360
- **Both have a mix of uses**
  - Aviation: Scheduled air carrier, air charter/taxi, general aviation
  - Information Technology: Transactional, communications, process control, graphics/text processing, and publishing
- **Both are a complex combination of people, processes, and technology**
- **Users/Customers of both have similar expectations of reliability**

The Big Difference – Risk Management

- **Aviation:** Errors and deficiencies result in death, injuries, brand impact and financial loss
  - **Risks are actively identified prior to deployment of any hardware or service** and positively managed in a risk profile
  - **All aspects of sources of risk are considered and controlled** through all phases of the life cycle of everything affecting flight operations:
    - design of hardware and software
    - manufacture of products used for aviation
    - qualifications and capability – current and ongoing – of all personnel directly involved in operations
    - absolute version and change control over all hardware and software
    - separation of duties for all critical decisions made by personnel
    - 100% accountability for all actions by operators and maintainers of equipment and critical operations
  - **Losses and incidents that could have created losses are required to be thoroughly researched** and *usually* positive measures are implemented to prevent reoccurrences
  - **Aviation product and service vendors experience immediate and often severe financial (and possibly legal) consequences** of any lapses in adherence with risk management

- **Information Technology:** Errors and deficiencies **result primarily in brand impact and financial loss**, although death and injuries are possible

How is the Aviation Risk Profile Managed?

- **Speed of adoption of technology**
  - New technologies are introduced slowly, only after substantial design and implementation reviews
  - Contrast this with the information technology philosophy of “ship it now, fix it later”
- **Regulatory environment**
  - All participants (pilots, controllers, mechanics, manufacturers, instructors, medical providers, passengers) are subject to active controls
  - The activities of the industry are monitored with a mandated feedback loop for improvements
  - Contrast this with the primarily voluntary compliance with industry-defined standards and unevenly enforced government standards in information technology
- **Training Standards**
  - All participants are required to undergo periodic education and almost all must periodically demonstrate proficiency
- **Operational Standards**
  - Deviations during execution that compromise safety are noted and investigated

What Can we Learn from the Aviation Industry?

- **Can we slow down the speed of adoption of new technology?** *No way!*
- **Can we create a more regulated environment?** *Probably not, but the management of compliance with the regulations already in place could be improved.*
- **Can we upgrade our training?** *Yes!*
- **Can we better manage our risk acceptance?** *You bet!*
- **Can we improve our operational activities?** *Absolutely!*

Risk Management

Managing Risk in Aviation

- **Aviation risk is managed in accordance with the "Safety Risk Management Policy" (SRM), as documented in US Department of Transportation Federal Aviation Administration, National Policy Order 8040.4A, effective 30 April 2012**

- **Impact is categorized into five categories:**
  - **Catastrophic:** Multiple fatalities
  - **Hazardous:** Multiple serious injuries, fatal injury to a relatively small number of persons (one or two), or a hull loss without fatalities
  - **Major:** Physical distress or injuries to persons, substantial damage to aircraft
  - **Minor:** Physical discomfort to persons, slight damage to aircraft
  - **Minimal:** Negligible safety Impact

- **Likelihood is categorized into five categories:**
  - **Frequent:** Expected to occur routinely
  - **Probable:** Expected to occur often
  - **Remote:** Expected to occur infrequently
  - **Extremely Remote:** Expected to occur rarely
  - **Extremely improbable:** So unlikely that it is not expected to occur, but it is not impossible

Aviation Risk Matrix

	Minimal Impact	Minor Impact	Major Impact	Hazardous Impact	Catastrophic Impact
Frequent	Acceptable	Acceptable with risk mitigation	Acceptable with risk mitigation	Unacceptable	Unacceptable
Probable	Acceptable	Acceptable with risk mitigation	Acceptable with risk mitigation	Unacceptable	Unacceptable
Remote	Acceptable	Acceptable	Acceptable with risk mitigation	Unacceptable	Unacceptable
Extreme Remote	Acceptable	Acceptable	Acceptable	Acceptable with risk mitigation	Unacceptable
Extremely Improbably	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable with single point of failure

Things to Notice on the Aviation Risk Matrix

- **The impacts and likelihoods are *pre-defined* and not subject to negotiation**
  - Interpretation, perhaps, but not negotiation
- **Risk acceptance is a defined part of the process, guided by the pre-defined impacts and likelihoods**
- **“Catastrophic” and “Hazardous” impacts have very little “wiggle room” on risk acceptance**
  - *Even “extremely remote” needs to be addressed!*
- **How can we adapt this approach to information technology?**

How Would we Characterize Impacts from an IT Perspective?

- **Catastrophic:**
  - Unrecoverable loss of a mission-critical IT system
- **Hazardous:**
  - Recoverable loss of a single mission-critical application with minimal recovery time
- **Major:**
  - Reduced/impaired service delivery to organizations/customers that prevent organizations and/or customers from achieving required or highly desired outcomes
- **Minor:**
  - Reduced/impaired service delivery to organizations/customers that limit the expected outcomes for organizations and/or customers
- **Minimal**
  - All impacts which don't fit into a category above

Let's just focus on *catastrophic*.

What are Examples of Catastrophic Impacts?

- **Catastrophic:**
  - Physical destruction of mission-critical IT asset, without possibility of recovery
  - Logical destruction of mission-critical IT asset by trusted actor (think rogue systems programmer) without possibility of recovery
  - Logical destruction of mission-critical IT asset by non-trusted actor (think malicious actor who has found a misconfiguration or vulnerability) without possibility of recovery
  - Logical compromise of a high-value mission-critical IT asset by trusted actor
  - Logical destruction of a high-value mission-critical IT asset by non-trusted actor
- **What are the counter measures that are needed to eliminate these risks?**
  - Effective physical security
  - Real-time redundancy
  - Demonstrable disaster recovery
  - Proper logical security
- **… and since these are catastrophic events, the risk matrix approach dictates that any non-"extremely improbably risk" must be addressed!**

What Logical Security Lapses Could Allow a Catastrophic Event?

- **Too many to list!**

  Some examples include:

  - Improper controls on resources which allow extraordinary access, such as System libraries (APF, System REXX, critical CLISTs, production batch jobs)
  - Improper network controls
  - Accidental introduction of malware by end-users (phishing attacks)

- **Think of all the counter-measures for all of these potential attacks.**

- **Since these are needed to eliminate the risk for a catastrophic event, *they must be done.***

Control techniques used in Aviation

Aircraft have only two states: Airworthy or un-Airworthy

An Airworthy aircraft is the result of:

- **Positive (required) multi-level inspections** of all critical system components by multiple trained (and actively licensed) personnel – annually, daily, before every flight and as dictated by mandatory maintenance inspection schedules for each specific model of equipment
- **100% compliance 100% of the time with all standards** – Type Certificates and Airworthiness Directives
- **Absolute version and change control** – all critical components are inspected, updated, maintained and/or replaced in compliance with either time in service, calendar time or operational cycles. There is no such thing as deferred maintenance or unsupported "versions".
- **Absolute hardware redundancy** when ANY single point of failure can be practically eliminated. The service condition of BOTH redundant systems must be operational at all times.
- **100% accountability for all activity involving the equipment** – accurate, complete and timely record keeping of all operations and maintenance must be in place before an aircraft is available for operations

Where could our systems be more like an Airworthy aircraft?

Information Systems Control Techniques

Some areas where our systems could be more like an airworthy aircraft:

- **Positive control of data access**
  - PROTECTALL(FAIL)
  - ERASE(ALL)
  - BATCHALLRACF
  - Backstop profiles on resource classes
  - Proper paranoid resource manager handling of SAF return code 4
- **Redundancy**
  - Effective use of Sysplex features and application features (such as a properly maintained, duplexed, and backed up RACF DB)
- **Integrity of the Operating Environment**
  - Operating system implementation that puts a loss of integrity of the operating system in the “Catastrophic” category
  - Effective matching of implementation and security policy
    - “The price of security is eternal vigilance”
- **Expectation of compliance**
  - Adherence to controls and risk management is monitored and enforced at the executive level

Reducing Risk by Learning from the Past

Learning from Mistakes Before they have a Big Impact

- **TWA Flight 514**
  - B727 (N54328) inbound to Washington National Airport from Columbus Ohio on 1 December, 1974
  - Diverted to Dulles airport due to high winds and vectored to a non-precision approach to runway 12 at Dulles.
  - While cruising at 7,000 feet the pilots were "cleared for the approach" into Dulles
  - The pilots began a descent down to 1,800 feet
  - Intense downdrafts caused minor (100-200 altitude deviations)
  - The aircraft impacted Mount Weather (summit 1,754 feet) at 1,670 feet, with first impact being 70' tall trees.
  - Eighty-five (85) passengers and seven (7) crew perish in the crash

Learning from Mistakes Before they have a Big Impact…

- **Investigation**
  - NTSB report determines that the primary cause is “Misunderstanding of orders or instructions”.
  - During the investigation, the NTSB discovers that **a United Airlines flight had made the exact same error six weeks earlier, but had recognized the error and recovered in time**. The investigation reveals that the **misunderstanding of “cleared for the approach” was widespread** and **that pilots were reluctant to report the confusion.**
  - The result of the investigation is the creation of the Aviation Safety Reporting System (ASRS).

Learning from Mistakes Before they have a Big Impact…

- **Aviation Safety and Reporting System (ASRS)**
  - A voluntary program which allows anyone involved in the aviation industry to report issues that will be investigated by an independent agency, the National Aviation and Space Administration (NASA).
  - Reports are anonymized when brought into the ASRS system to preserve the confidentiality of the reporter.
  - Reporters have an incentive to report issues:
    - If the FAA independently detects an issue and takes an action, if the person under investigation is “guilty”, and if the person had reported the issue to the ASRS, the penalty will be waived. Key provisions:
      - No limit on the number of reports,
      - Can be used to waive a penalty once per five years, and
      - Cannot be claimed if the action was illegal or willful (loses anonymity as well).
  - **NASA analyzes trends and makes recommendations. <u>Many of these have been adopted by the FAA.</u>**
  - Publishes monthly two-page report called “*Callback*”.

Learning from Mistakes Before they have a Big Impact…

- **Aviation Safety and Reporting System Intake in November, 2015**

Air carrier/Air taxi pilots:	4,591
General aviation pilots:	1,047
Flight attendants:	507
Controllers:	434
Military/Other:	232
Dispatchers:	206
Mechanics:	171
Total:	7,208

Lockheed C-140 Jet Star

- **Question:** *Why can't we have an ASRS-like process in our environments?*

Learning from Mistakes After they have a Big Impact

- **United Airlines 232**
  - B727 (N54328) inbound to Chicago O'Hare from Denver Stapleton on 19 July 1989 with 296 onboard
  - 57 minutes into the flight, the fan disk of its tail-mounted GE CF6-6 engine disintegrated. The shrapnel from the disintegration punctured all three hydraulic lines, rendering the ailerons, elevator, and rudder inoperative.
  - The crippled airliner landed at Sioux City, Iowa
    - … with 185 surviving the ensuing crash

Learning from Mistakes After they have a Big Impact…

- **Why Were there So Many Survivors?**
  - UAL 232 pilot-in-command Captain Al Haynes attributes the high survival rate to:
    - **Cooperation and communication**
      - The crew was trained on Crew Resource Management (CRM) techniques encouraged all members of the flight crew to share information and expertise
    - **Preparation**
      - Just the day earlier, Sioux City had performed a drill that was very similar to the actual crash
    - **Luck**
      - The flight was during daylight and the weather was good
      - The accident occurred at a shift change
      - Simulations of the accident with over 50 equivalently-trained crews resulted in no better outcome
- **What was learned?**
  - CRM works!
  - Aviation instrumentation was upgraded to allow flight management systems to successfully complete a landing under similar conditions.

Parting Thoughts

- While the urgency and obvious necessity of risk management in aviation will likely eclipse the perceived need for such measures in information technology, are the concepts and many of the tools and techniques that have been developed in over a century of aviation applicable to strengthen information technology?
- How many positive controls that are available now in information technology that do reduce risk are not being implemented for reasons that would not logically be possible in aviation?
- What is really preventing the implementation of some of the available controls we all know would reduce risk (think of the areas in the aviation risk matrix that MUST be addressed)?
- Would the adoption of an aviation-type risk management approach for information technology generate positive outcomes, such as being more competitive in the marketplace, for you and/or your organization?
- How can we work together to increase the awareness of how risk management can be improved for information technology?

Please do not attempt to fly your systems, but please do strive to make your systems more like an airplane!