PHARMACEUTICAL ONLINE

Guest Column | November 15, 2019

People: The Most Persistent Risk To Data Integrity

By Kip Wolf, Tunnell Consulting, @KipWolf

In modern times, the business operating model is commonly referred to by the three resources of "people, process, and technology." Business intelligence (BI) activities also frequently refer to the triangulation of "people, process, and technology." And the triad of "people, process, and technology" is touted by organization change management (CM) pundits and business process management (BPM) experts alike. It is said that these maxims stem from an article by Harold J. Leavitt, *Applied organisational change in industry: Structural, technological and humanistic approaches*, that first appeared individually and in textbooks in the mid-1960s. And these concepts were clearly incorporated into countless titles over the decades since, including many recent books.[1-8]

People, Process, And Technology In Data Integrity

When considering the data integrity condition of an organization, we often use this structure to perform our analysis and to inform our presentation of the results. However, by the time the analysis is concluded, the operational conditions within the relationship of these three resources has changed. The results of any evaluation are limited to a snapshot of data — a brief glimpse of the conditions at a particular isolated point in time — as these resources are ever-changing individually and in their relationship to one another. In most cases, the topics are considered in terms of how to integrate these three resources. Let's consider their individual impacts on data integrity.

Technology

Working backward, we first consider technology. Technology and, in particular, information technology, continues to advance at an exponential rate. Some tech pundits even go so far as to suggest that technology "will evolve to the point where it will know more on an intellectual level than any human"[9] within the next 25 years. While these perspectives may be on the fringe, they represent some of the extreme examples of the rapid advancement of technology.

21 CFR Part 11 was written with a heavy focus on information technology and we in the life sciences industry have been keenly focused on information technology for many decades. Computer system validation and change control are our primary tools for limiting information technology variability in our operations. We rely on these controls to manage change and variability in our technology in operations, and we are generally well educated on the requirements and methods to do so.

Process

Next, we consider process management. Process variation is something with which we are also very familiar in life sciences, as there has been much application over the last few decades of Lean Six Sigma to limit process variation. In addition, there has been much application of technology solutions for control and digital optimization using BPM tools such as Promapp, Kissflow, and ProcessMaker. While overhead is required to manage such tools, they provide great benefits in overall process understanding that lends positive results to limiting process variation.

People

Variation in personnel resources remains the greatest risk to our operations and specifically to data integrity. As cultures change or are blended/mixed over international business operations, we realize ever-changing and evolving behavior in our people. Differences also exist in the expectations from generation to generation. As new generations join the workforce, new cultures emerge that present differing expectations of the workplace.

Gilbert's Behavior Engineering Model (BEM) presents a concise way to consider both the environmental and the individual influences on a person's behavior. The model suggests that a person's environment supports impact to one's behavior through information, instrumentation, and motivation. Examples include feedback, tools, and financial incentives (respectively), to name a few. The model also suggests that an individual's behavior is influenced by their knowledge, capacity, and motives. Examples include training/education, physical or emotional limitations, and what drives them (respectively), to name a few. Let's look at some further examples to better

- “Analyst … explained that he deletes older data to make space for newly acquired data.”
- “You permanently deleted the first five sample injections. You then renamed the last two injections and reported that they met specifications.”
- “Analysts manipulated and deleted audit trails.”

Knowledge limitations may present themselves through changing operational needs. When processes or technologies are improved, the individuals likely need to be retrained to keep pace with the improvements. In some cases, we have seen individuals fall short of maintaining the necessary knowledge. In such cases, these knowledge gaps may create risks to data integrity (e.g., failing to understand and execute appropriate audit trail review).

Capacity limitations may present themselves by straining the existing workforce. When overtime is required and approved, individuals may work beyond their physical and emotional limits. We have seen this lead to data entry errors, information review mistakes, and operational failures. We have people with good intentions cause catastrophic failures by pushing themselves beyond their physical and emotional capacity.

Motive limitations may present themselves as failures due to malice or plain ignorance. We have seen negative impacts on corporate brands by disgruntled employees motivated by anger who publicly share sensitive information in negative ways. We have also seen people make mistakes simply by not considering the consequences of their well-intentioned actions. For example, an operator driven by a motive to please their superiors, when questioned about the incorrect label on a piece of equipment in the manufacturing suite, quickly overwrote the batch number on the vessel to make the correction (promptly causing an investigation).

Making Good Progress, Only To Start All Over Again

Regardless of the maturity of an organization’s data integrity practices, the people component remains the greatest risk. Consider an organization that has evolved to a high degree of data integrity and quality culture maturity, but then it changes and realizes basic risks all over again. When brand-new junior staff are hired or organizations are merged as a result of acquisition, the organization frequently has to start all over again or at least consider readdressing some basic data integrity needs with its new and combined staff.

The important thing for individual contributors, operational managers, and executive leaders to remember is that data integrity evolves. What works today may not work tomorrow. We must constantly evaluate and consider adjusting our strategies for data integrity. One of the most overlooked areas is our human resources – our people. We must consider how our changes in human resources impact our overall data integrity, from an individual change with a single new hire to a departmental or corporate level change with a merger or acquisition (see “What Your Organizational Design Says About Your Commitment To Data Integrity”). Change impact analysis is a valuable activity, not just during formal change request processes. We find that the most effective managers of data integrity consider change impact analysis as part of their critical thinking skills. Whether informally thinking about “best-case/worst-case” or more formally discussing scenarios in a process failure mode and effects analysis (FMEA), embedding continuous critical thinking of and by the people resources in your organization may greatly improve the conditions of this most persistent risk to data integrity.

References:

1. Jack S. Goulding and Farzad Pour Rahimian, *Offsite Production and Manufacturing for Innovative Construction: People, Process and Technology*, Routledge, Jun. 25, 2019.
2. Diane Updyke, *Building Your Sales Team: Beyond People, Process, and Technology*, THiNKaha, Mar. 11, 2019.
3. Jason Sachowski, *Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise*, CRC Press, May 23, 2018.
4. Judah Phillips, *Building a Digital Analytics Organization: Create Value by Integrating Analytical Processes, Technology, and People into Business Operations* (Paperback), Pearson FT Press, Nov. 25, 2017.
5. David J. Piasecki, *Inventory Accuracy: People, Processes, & Technology*, OPS Publishing, Mar. 15, 2003.
6. Kan Wang, *People, Process, and Technology Management Framework: A Manager's Practical Guide to Establishing a Structure for Growth*, CreateSpace Independent Publishing Platform, Jul. 23, 2011.
7. Dean Lane, *The Chief Information Officer's Body of Knowledge: People, Process, and Technology*, Wiley, Sep. 13, 2011.
8. *The Toyota Product Development System: Integrating People, Process And Technology*, by James M. Morgan and Jeffrey K. Liker | Mar 25, 2006
9. John Brandon, “An AI god will emerge by 2042 and write its own bible. Will you worship it?”, *VentureBeat*, Oct. 2, 2017.

About The Author:

Kip Wolf is a principal at Tunnell Consulting, where he leads the data integrity practice. Wolf has more than 25 years of experience as a management consultant, during which he has also temporarily held various leadership positions at some of the world’s top life sciences companies. Wolf temporarily worked inside Wyeth pre-Pfizer merger and inside Merck post-Schering merger. In both cases he led

Kip.Wolf@tunnellconsulting.com.

Comments (3)

Login

Sort by: **Date** Rating Last Activity

domfurniss 0p · *4 weeks ago* +3

Thanks for highlighting these issues. However, IMHO I think it overemphasises the role and responsibility of individuals at the sharp-end, verging on blaming them for errors, e.g. because people have chosen to work beyond their emotional and physical limits. I'd push back a little and ask why the organisation has put people in this position. Risks emerge from the system. Latent conditions away from the sharp-end can foster error. From a Human Factors perspective we would focus less on blaming people for error, and make 'the system' shoulder more of the responsibility for the risks created. Is work organised well so people find it easy to do the right thing, hard to do the wrong thing, and almost impossible to do something really bad? Look at the usability of data entry systems, design of tasks and procedures, meaningful checks, reminders, good use of technology and involve the workforce in improvement processes so they have involvement in redesigning systems that work well for them.

For example... it seems this analyst is working with a technology that simply doesn't have enough space for the job, so they have to do extra work to capture new data and keep the whole system working and moving forward. “Analyst ... explained that he deletes older data to make space for newly acquired data."
This isn't a people problem, it's a technology and organisational problem. Sometimes there is good reason for non-compliance.

Turning the title on its head a little... let's work with people to strengthen good system design and practices rather than see them as the problem.

Reply

kipwolf 24p · *3 weeks ago* +3

Thanks Dominic! Good points! I agree and am passionate about human factors, system usability/UX, and management behavior. In fact, I train on individual behavior awareness and how to help prevent human error by being self aware, understanding your limitations and communicating them clearly with your management. I agree as does FDA that the responsibility for the Quality Culture is on management. “It is the role of management with executive responsibility to create a quality culture where employees understand that data integrity is an organizational core value and employees are encouraged to identify and promptly report data integrity issues.” - FDA Guidance for Industry, Data Integrity and Compliance With Drug CGMP, DEC 2018

Reply

Amol Arankar · *2 weeks ago* +1

I agree with you Kip that wherever systems are not fully automated (which is the case with an average pharma company) the most vulnerable factor remains to be people. Technology and processes need maintenance but these can definable and definite but people's motivation, job satisfaction depend on personal as well as organizational factors which are complicated and are not that easy to control. Add to it the factor of change in personnel at various levels including those who are critical for generation and handling of data. So in my opinion people including the management are the most persistent risk to data integrity.

In my opinion technology and processes contribute to IQ of an organization but it's people who not only contribute towards IQ but towards EQ of an organization as well. And we know that we cannot ignore EQ.

Thanks

Reply

Post a new comment

Enter text right here!

Comment as a Guest, or login:

Name

Displayed next to your comments.

Email

Not displayed publicly.

Website (optional)

If you have a website, link to it here.

Subscribe to None

Submit Comment

YOU MAY ALSO LIKE...

To Err Is Human: Contextual Communication’s Impact On Data Integrity

Despite the best efforts of those responsible for data integrity, the potential for human error is directly and indirectly impacted by the corporate, the national/regional , andquality culture of an...

Data Integrity, Deviations, And Shop Floor Quality

Continuous improvement in data integrity can advance a firm on the journey toward a mature culture of quality, particularly through the implementation of QA on the shop floor. Batch record review...

Data (Integrity) Pirates: Preventing And Detecting Malicious Intent

During a recent meeting of data integrity professionals, a fundamental question was posed by a member of the group: "How can one prevent or detect malicious intent as it relates to changes to...

Startups, Cloud Storage, & Data Integrity: Don't Let This Happen To You!

Data integrity is of paramount importance to ensure patient health and safety and to improve shareholder value, particularly for virtual companies. Startups finding themselves in the throes of...

The 5 Basic Tenets Of Data Integrity — And How Failures Occur

AI, Data Integrity, & The Life Sciences: Let's Not Wait Until Someone Dies

When And How To Implement Data Integrity Practices In The Product Development Lifecycle

Cheating In The Lab: 3 Data Integrity Pitfalls To Avoid In Laboratory Operations

Strong Data Is Generated By Strong People

What Is The Link Between Quality Metrics, Data Integrity, And Quality Culture?

Comparing Recent Data Management/Integrity Guidances From MHRA, WHO, & PIC/S

Advertise
Ad Specifications
Request Media Kit

Subscribe
Newsletter

Life Science Connect
BioProcess Online
Biosimilar Development
Cell & Gene
Clinical Leader
Drug Discovery
Laboratory Network
Life Science Leader Magazine
Med Device Online
Outsourced Pharma

Editorial
Archived Newsletters
Article Reprints
Editorial Submission Guidelines
Editorial Contributors

Events
CMO Leadership Awards
CRO Leadership Awards
Outsourced Pharma Events

Training
Life Science Training Institute

Learn More
About Us
Contact Us
Work For Us