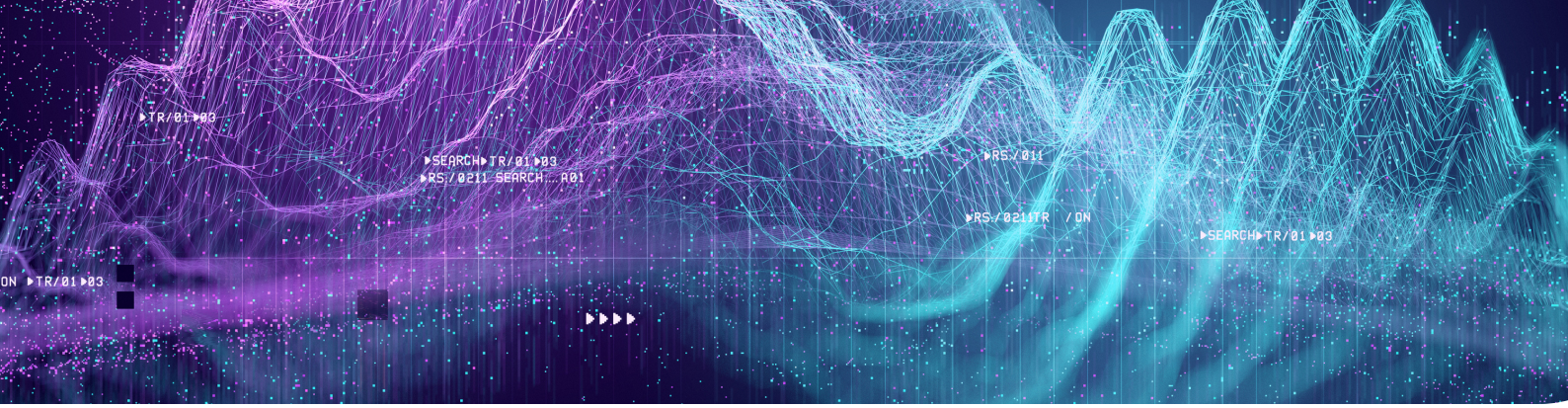
Bioanalysis ZONE

Implementation of automation, IT support and cybersecurity in bioanalysis

fsg

In association with:

Alturas Analytics, Inc.
The LC-MS Experts



Contents

Technology Digest: implementation of automation, IT support and cybersecurity in bioanalysis

by Naamah Maundrell
(Editor-in-Chief, Bioanalysis Zone)

The use of automation in the bioanalytical laboratory

Automated tools and platforms have benefited the bioanalytical laboratory by reducing method development and data turnaround times. Simultaneously, automation has increased throughput, data integrity and overall productivity. These benefits have led to reduced costing and drug development timelines enabling drugs to get to patients faster, which is the ultimate end goal [1].

Over the past 2 years, research goals and timelines have remained unchanged meaning it was essential for companies to continue operating as usual, finding innovative ways to overcome the unprecedented challenges of the COVID-19 pandemic and to deliver quality data to clients on time [2,3]. During this time, the bioanalytical industry encountered many challenges particularly for IT support, including national lockdowns, stay-at-home orders, a surge of cyberattacks and supply-chain issues [3]. As onsite staff schedules were staggered, remote working increased the value of a robust IT system. The maintenance of an accessible data interface system that allows the sharing of information, database integration and generation of metrics and reports, was now more important than ever [2]. Companies realized the significance of investing in bioanalytical automated platforms that link to robust IT systems, with businesses continuing to innovate these technologies post the COVID-19 pandemic [1].

For laboratory automation to be successful, automated technologies are required to be integrated into a laboratory information management system (LIMS) to streamline reporting and data analysis [4]. It is necessary for companies to have an automation strategy whereby the integrated systems are periodically updated to cater for the developing laboratory needs. Key drivers for electronic laboratory notebooks include standardized working practices, increased speed of data review, productivity and decision-making. When implementing an electronic system data integrity and regulatory compliance are essential [5]. There are different integrated LIMS systems – developed by equipment vendors – that are designed to assist laboratories in sample management, data processing, evaluation and reporting [4]. Some examples of core data systems, which are used for business' day-to-day operations, include: SCIEX Analyst™, Thermo Fisher Scientific Chromeleon™, Thermo Fisher Scientific Watson LIMS™ and Certara WinNonlin™. Furthermore, Alturas Analytics developed an in-house custom electronic laboratory notebook termed Holmes [3].

The Holmes database can audit all materials used in each batch, monitor pipette verification and is 21 CFR Part 11 compliant with all reference standards. Reagents are assigned unique bar codes allowing review and tracking of original component items and the system also assigns bar codes to calibration standards, QCs and solutions. The electronic system tracks drug concentrations, quantities, storage locations, used equipment and complements the Thermo Fisher Scientific Watson LIMS™, which mainly tracks unknown samples [2]. Bo Cheng, PhD, Director of Information Technology at Alturas Analytics (ID, USA), commented on the challenges of electronic systems and records:

> *There are two challenges associated with electronic systems and records. One is 21 CFR Part 11 compliance. In order to be compliant, all record creating and modification must be signed off with electronic signature and audit trailed with who, when, where, what and reason for the change. The second is the fact that the Holmes (formerly Chemical Inventory Management System (CIMS)) system is not an OTS (Off-The-Shelf) software application. It is a user workflow driven, purpose-built in-house application. The end users expect the software to be tailored to the exact workflow in the lab. To accomplish those, the designer has to have excellent understanding of FDA regulations and the lab operations. These also add to the complexity of the design and coding of the application.*

How companies adapted during the COVID-19 pandemic

A global challenge of maintaining full operations throughout the pandemic was the restriction of onsite staff numbers. To overcome this, companies implemented detailed schedules and resources to ensure study progress. IT support played a pivotal role in employing project management software that enabled the tracking of available personnel who were onsite versus offsite. During the restrictions, IT departments also maintained remotely accessed software that provided information on current project metrics, batch runs, invoices and contracts in real-time [6].

However, not all companies had the resources to develop in-house automation capabilities, which lead to increased outsourcing due to cost and capacity limitations [1]. At Alturas Analytics, the IT department adapted quickly by provisioning additional equipment, VPN access and higher bandwidth to allow remote working, regulatory inspectors and auditors to conduct virtual audits [3].

> *We implemented or expanded the use of multiple online communication platforms, such as Zoom and Teams, in order for communication among staff and collaborations with sponsors working remotely to continue uninterrupted. We also increased our internet bandwidth and acquired additional VPN authentication devices. Relevant security and compliance policies were updated and SOPs revised as applicable. Our IT and Quality Assurance Units introduced the ability to conduct virtual audits. Additional wireless hotspots were installed throughout the operation in order to accommodate interactive facility tours* – commented Jennifer Zimmer, PhD, Laboratory Director, Alturas Analytics (ID, USA).

The new normal of remote audits

The COVID-19 pandemic disrupted supplier and regulatory audits, and out of necessity due to travel restrictions, remote inspection approaches were developed [7,8]. Importantly, the regulatory laboratory inspection basics did not change, still consisting of analytical data and supporting documentation reviews, and discussions with site staff conducting the studies.

Remote inspection approaches utilized portals and IT systems to effectively transfer electronic data and supporting documents. Video conferencing facilities enabled virtual laboratory tours, aided by using good quality video equipment, hand-held gimbal devices to stabilize the camera and Bluetooth speakers [7]. Although technology and IT support propelled the ease of virtual audits, key challenges remained including the time spent requesting and accessing data, poor internet connection as well as conflicting time zones [8].

Alturas Analytics hosted the first remote FDA audit on 14 April 2020, which lasted 16 business days [7]. Through sharing knowledge and experience a useful virtual audit checklist was compiled, highlighting that clear communication with the authorities before the audit is essential, to understand the documentation required and the platforms that will be used [3].

The prominence of cybersecurity

While IT departments strive to be agile and adaptive, cybersecurity remains a high priority to protect clients' intellectual properties. A company's IT support is vital to alert any cyberattacks and system vulnerabilities, to patch systems, conduct user awareness training and implement filtering and anti-malware technologies for emails [3]. A cybersecurity aware culture should be fostered with periodic user awareness training and security policy [9].

Unfortunately, an increasingly common term used over the last few years is ransomware, which is the infiltration of malware into a corporate network. This then encrypts files meaning the business ceases to operate due to inaccessibility of the encrypted files. The threat actor usually demands payment for decrypting the files or warns that the confidential information will be made public. As IT systems are a crucial part of the bioanalytical laboratory it is important to have a preventative action plan to reduce the risk of ransomware attacks ensuring employees follow best practices to avoid infiltration [9].

For example, Alturas Analytics contracted an external security consulting firm to conduct internal and external penetration tests, to assess cybersecurity policies and implementations by Federal Government standards (NIST Cybersecurity Framework). This meant that the IT infrastructure, environment and policies were secure and resilient [3]. Bo Cheng remarked on the prevention of ransomware:

> *"The prevention of ransomware involves the entire company and heavily relies on ordinary employees' daily activities at their workstations. No technical measures taken by IT will provide 100% protection."*

Summary

As technologies and platforms continually improve and innovative current practices, it is paramount that automation is required to improve quality, timelines and return on investment. To optimize the drug-development process, companies need to be able to acquire, integrate and disseminate data to make strategic decisions [2]. Cybersecurity remains a high priority to protect clients' intellectual properties and requires continuous improvements to avoid cyberattacks and system vulnerabilities. As companies adjust to a new normal post COVID-19 restrictions, it is likely that hybrid inspection programs will remain going forward as remote audits have been an effective tool and the industry has seen big improvements in technology [8]. Overall, automation needs to be embraced by the whole industry to allow everyone to benefit [1].

References

1. Li M. Bioanalytical laboratory automation development: why should we and how could we collaborate? *Bioanalysis*, 7(2), 153–155 (2015).
2. Bioanalysis Zone. eBook: the use of automation in the bioanalytical lab. (2021): https://www.bioanalysis-zone.com/ebook-the-use-of-automation-in-the-bioanalytical-lab_alturas_gyros/
3. Bioanalysis Zone. In the Zone: virtual audits. (2021): https://www.bioanalysis-zone.com/in-the-zone/in-the-zone-virtual-audits_itz_alturas/
4. Patel V, Leach D, Hornberger M *et al*. Automating bioanalytical sample analysis through enhanced system integration. *Bioanalysis,* 5(13), 1649–1659 (2013).
5. McDowall RD. Developing a strategy for a regulated electronic bioanalytical laboratory. *Bioanalysis*, 6(2), 165–184 (2014).
6. Bioanalysis Zone. Ask the Experts: how business continued through the COVID-19 pandemic. (2020): https://www.bioanalysis-zone.com/ask-experts-business-continued-covid-19-pandemic__ate_covid_alturas/
7. Alturas Analytics. Are Remote Audits Here to Stay? (2021): https://alturasanalytics.com/media/50962/2021_alturasanalytics_landolakes_dschumacher.pdf
8. Wakelin-Smith J, Vinter S. Conduct of remote inspections: challenges and progress. *Bioanalysis*, 13(24), 1789–1791 (2021).
9. Alturas Analytics. AAPS eChalk Talk: Today's Challenge in Cyber Security – Defending Against Ransomware. (2021): https://alturasanalytics.com/media/50992/ransomware-aaps-echalk-talk-bo-cheng.pdf

Disclaimer
This article has been drawn from the discussions from the Technology Digest article published in Bioanalysis Zone, which was sponsored by Alturas Analytics. The opinions expressed in this feature are those of the author and do not necessarily reflect the views of Future Science Group.

Financial & competing interests disclosure.
N Maundrell is an employee of Future Science Group and Editor-in-Chief of Bioanalysis Zone. The author has no other relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript apart from those disclosed. No writing assistance was utilized in the production of this manuscript.

This feature has been brought to you in association with Alturas Analytics. The opinions expressed in this feature are those of the author and do not necessarily reflect the views of Bioanalysis Zone or Future Science Group.

For reprint orders, please contact: reprints@future-science.com

Bioanalysis

Conduct of remote inspections: challenges and progress

Jason Wakelin-Smith*,[1] & Stephen Vinter**,[2]

[1]Medicines & Healthcare products Regulatory Agency (MHRA), Library, National Institute for Biological Standards & Control (NIBSC), Blanche Lane, South Mimms, Potters Bar, Hertfordshire, EN6 3QG, UK

[2]Inspection, Enforcement & Standards, Medicine & Healthcare products Regulatory Agency, 10 South Colonnade, Canary Wharf, London, E14 4PU, UK

*Author for correspondence: jason.wakelin-smith@mhra.gov.uk

**Author for correspondence: stephen.vinter@mhra.gov.uk

First draft submitted: 2 November 2021; Accepted for publication: 2 November 2021; Published online: 17 November 2021

Keywords: compliance • inspection • MHRA • pandemic • remote

Jason Wakelin-Smith

Jason joined the MHRA in November 2006 as a GCP Inspector, became a Senior Inspector in 2015 and a Lead Senior Inspector in 2017. Jason has a split role between the GCP and laboratories inspection teams within the MHRA conducting a variety of inspections including GCP inspections of trial sponsors, CROs and analytical laboratories, bioequivalence trials as well as conducting GLP inspections as part of the UK GLP Monitoring Authority.

Jason has a BSc (Hons) in Biomedical Science and a Postgraduate Diploma in Pharmaceutical Technology & Quality Assurance. Prior to joining the MHRA Jason spent seven years in the UK National Health Service working in hospital pharmacy.

Stephen Vinter

Stephen is Operations Manager for the GLPMA and Laboratories Group at the MHRA and is Head of the United Kingdom Good Laboratory Practice Monitoring Authority.

Prior to joining the Agency in 2012, Stephen worked in Operations Management at a CRO. Stephen has also worked in the manufacturing sector and is a Chartered Chemist and Chartered Quality Professional.

In his role as a Lead Senior Inspector, Stephen conducts GCP and GLP inspections of organizations and laboratories within the UK and overseas facilities as part of the MHRA inspection program for organizations conducting Bioequivalence studies. He has worked on several regulatory guidance documents and represents the Pharmaceutical Inspection Co-operation Scheme as an observer on the ICH M10 Expert Working Group.

How have the methods of inspection changed to maintain regulatory standards despite the restrictions faced by both laboratories & regulatory bodies over the course of the pandemic?

We had the same challenges as all organizations during the pandemic, and the most significant challenge being the inability to travel unless for a critical reason. Laboratory inspections over the pandemic have, by necessity, become more focused with inspections reprioritized to those supporting the development of COVID-19 vaccines and treatments alongside our normal inspection programs. Our first goal was to develop remote approaches to allow us to continue our inspection programs during travel restrictions.

Even before the pandemic within the wider Inspectorate, we had started to use office-based inspections as part of our inspection processes. For example, we would often carry out the first day of a GCP inspection remotely, to review data or information requested in advance so as to maximize our time on site. We were also running a pilot of focused pharmacovigilance inspections that was entirely office based. Across the Inspectorate we had started to develop some of the basic tools and techniques necessary to conduct remote inspections so we felt we were in a strong position at the start of the pandemic to implement a suitable remote inspection program in our team.

newlands press

A key aspect that has been worked on for several years across industry and the MHRA has been the development of effective tools for the transfer of electronic data and documents to support inspection activity. When we started developing remote (or office based) inspections, we would often use portals or commonly available platforms provided by the organization being inspected supported by video conferencing facilities and remote access to electronic systems where this could be supported by the organization being inspected. The MHRA have introduced the use of Microsoft® Teams as our inspection platform, which has permitted the integration of file sharing, the conduct of interviews via videoconference and online chat between the inspectors and inspection host into a single platform.

The basics of laboratory inspection have not changed during the pandemic; they continue to consist of reviews of analytical data and supporting documentation alongside discussions with site staff to understand the systems and processes that underpin the conduct of the study analysis. Some aspects of traditional surveillance style inspections are harder to carry out such as tours of facilities or readily available access to laboratory systems where a degree of technical support or infrastructure is required. We have conducted several bioequivalence inspections during the pandemic and at each have managed to undertake tours of the clinical and bioanalytical facilities supported by the site staff using mobile phones or tablets, microphones and with willing assistants to act as the camera crew!

Probably the biggest changes have been associated with the adoption of electronic ways of working wherever this can be supported. We have changed the type and format of data that we request allowing the transfer of data onto our MS Teams platform and subsequent data review using our own software. We have also requested remote access to any electronic systems at the laboratory from our desktops where possible, and where this not possible then we use shared desktop sessions to allow us to interact with software.

We have identified significant findings during remote inspections, so, although they have their challenges, remote inspections are an effective tool and one which is likely to remain as part of a hybrid inspection program going forward. They work well for focused inspections, for example to follow-up to specific issues, CAPA review or those that are very data orientated.

What have been the key challenges of conducting regulatory inspections amidst a global pandemic?

We have to recognize that it is not just the inspectors that have been forced to work remotely but also the companies themselves so we have made sure that staff at the organizations being inspected were not making unnecessary journeys traveling into the laboratory or office purely to access documentation on our behalf and potentially putting themselves (and others) at risk during the process. We have not experienced significant issues with accessing staff, data or documentation but we suspect there have been plenty of people behind the scenes trying to provide us with access to the information we require whilst complying with pandemic related restrictions.

How easily can inspection protocols & assessment criteria be adapted to remote inspections?

Readily – once we have appropriate access to staff, data and documentation then the inspection is conducted in a similar manner to that of an on-site inspection minus the *ad hoc* face-to-face interactions.

What are the key challenges of conducting remote inspections from a regulatory perspective?

It takes a little longer to conduct a remote inspection, we may not spend so much time traveling, but the time spent accessing, requesting documentation, asking questions and obtaining clarifications, can take longer. We recognize this when we schedule inspections and also take into account that we can sometimes be in different time zones.

Technology is incredibly important. Poor internet connections can cause significant problems with video conferencing, facility tours and access to data, and this is something that is discussed with the organization during inspection planning.

We have also been challenged by the number of systems that we need to gain access to in order to inspect the selected processes remotely and in full along with the ability of the organization to grant us remote access to these. From a laboratory perspective, we have seen a lot of instrument platforms which are not networked let alone set up for remote access by an external organization along with compartmentalized access to broader systems such as those containing standard operating procedure or training records.

There are also plenty of paper-based processes in place within some of the laboratories we have inspected, which may require scanning before they can be provided to us for review. This is often not just associated with the trial or study records but also any supporting logbooks and equipment records.

All these challenges are discussed during planning with the facility to allow us to reach a suitable solution that works for the inspectors and the facility.

Are there any advantages of remote inspections over traditional face-to-face inspections?

They have a place in the inspector's toolbox for focused assessment of particular aspects of a study, such as the review of analytical data. We have copies of various types of analytical software at the MHRA which enables us to inspect the data remotely in our own system without causing an increased burden on the laboratory by us having to be on site to conduct this part of the inspection. Certainly, with inspections overseas there is a greater flexibility found when trying to schedule inspections with the laboratory as complex travel requirements are not required!

Do you have any advice for laboratories on best practice when preparing for a remotely conducted inspection?

It is important to discuss with the lead inspector as early as possible about how the inspection will be conducted remotely. These discussions during the planning phase ensure the inspection platform is set up accordingly to allow a smooth exchange of information, to schedule the various interviews and tours required and also to conduct checks on the system performance before the inspection starts.

Make sure that you understand the data flows associated with the studies selected for inspection and work out how access to the analytical data and supporting metadata, such as audit trails, can be given. This may be in the form of remote access to your systems, transfer of data for review using software held by the MHRA or agreement that guided access may be the only possible route available (although this is not ideal and should be discussed with the lead inspector). Ultimately, the inspector will want to follow the generation of data from the source documentation through to its eventual inclusion in the study report via all of the transfers and transformations it goes through.

Identify what records are likely to be required in order to support the inspection. If you are unsure what is likely to be required, then a discussion with the lead inspector is always encouraged early in the process of setting up the inspection.

If remote tours are to be conducted then ensure sufficient Wi-Fi coverage exists throughout the facility and consider the use of a 'presenter' for the tour who is provided with a microphone and the ability to hear the inspection team with another member of staff operating the camera.

Do you think remote inspections will reshape the future of the bioanalytical regulatory landscape, to become the 'new norm'

It is likely that the 'hybrid' inspection model, with inspections consisting of both remote and on-site components, will continue after the pandemic. Improvements in technology are likely to increase the use of remote tools, making the inspection more efficient for both inspectors and the laboratory alike.

– This interview was conducted by Sankeetha Nadarajah, Managing Editor of *Bioanalysis*.

Financial & competing interests disclosure

The authors have no relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript. This includes employment, consultancies, honoraria, stock ownership or options, expert testimony, grants or patents received or pending, or royalties.

No writing assistance was utilized in the production of this manuscript.

Bioanalysis ZONE

Alturas Analytics, Inc.
The LC-MS Experts

Infographic: The ultimate remote audit checklist

IN THE ZONE
Bioanalysis ZONE

Alturas Analytics, Inc.
The LC-MS Experts

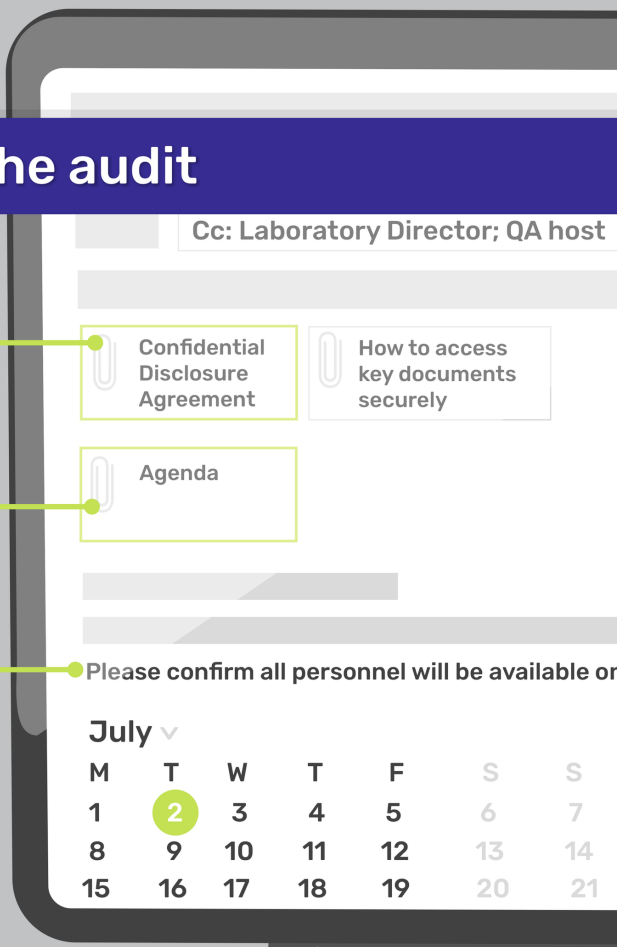
The ultimate remote audit checklist

Communication before the audit

1. Ensure a CDA is in place for all participants.
2. Prior to a sponsor audit, an agenda should be received acknowledging who will be participating in the inspection and stating the scope of the audit.
3. Communicate the desired date with the auditor. Confirm appropriate scientific personnel, Laboratory Director and QA host are available for the remote audit.
4. Explain to the auditor an overview of how remote audits are typically conducted.

Example:

**"PDF copies of key documents will be placed onto an online secure folder accessible to the auditor. Access to documents is typically granted five business days prior to the inspection to allow the auditor to prepare beforehand.
The actual meeting will begin with a video conference meeting, so please be prepared with a computer that has a video camera and microphone (or dial in via phone).
We also provide a live virtual lab tour, during which the auditor will be able to ask questions."**



Preparing for the audit

1 Establish an online file sharing website for the placement of documents the auditor will need to access. Also agree on the dates of access to be granted to the auditor.

2 It is recommended to upload the following documents:

- Audit agenda
- Master schedule of sponsor studies
- Organization chart
- CVs, job descriptions and training for key individuals
- SOPs
- Forms
- Additional documents requested by auditor prior to or during visit
- Facility audit schedules
- Expected studies to be reviewed
- Regulatory inspection history & permits (e.g., FDA registration)
- Technical procedures
- Floor plans

3 Establish a video conferencing meeting invitation and include all participants.

4 Ensure a tour leader and videographer are designated for the lab tour and an approximate time is established. Practice the lab tour using the camera and anti-motion gimbal using the video conferencing platform.

5 Review previous audit report for follow-up discussions and the questionnaire/survey if one was completed recently.

6 One business day prior to the remote audit ensure SOPs and other documents in the file sharing site are current. Note if any revisions will be coming into effect during the audit.

7 Review the introductory presentation to ensure it is current prior to the audit. Create a PDF that is ready to email to the auditor at the conclusion of the presentation.

During the audit

During the lab tour:

- Speak loudly and clearly
- Walk slowly to provide a clear view of the facility
- Leave time for questions as you go
- To improve viewers experience use a Bluetooth microphone/speaker and a cell phone held with an anti-motion gimbal

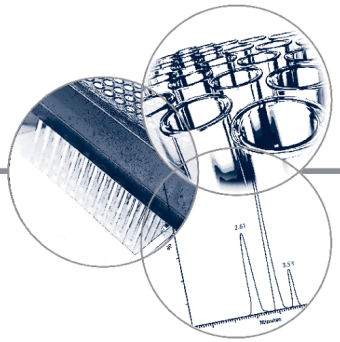
- Keep a detailed record of audit notes that capture significant times, requests, breaks and observations throughout the audit.
- Take into account extra time may be needed if connectivity problems occur.
- Near the conclusion of the audit, the auditor may indicate the time for the close-out. Relay that information to appropriate personnel.
- At the close of the audit, finalize the audit notes and share with appropriate personnel. Secure all documents that were shared online.

IN THE ZONE Bioanalysis ZONE

This infographic has been created as part of a Bioanalysis Zone feature in association with Alturas Analytics.

Alturas Analytics, Inc. The LC-MS Experts

PERSPECTIVE



Developing a strategy for a regulated electronic bioanalytical laboratory

This perspective article considers the strategy, design and implementation of an electronic bioanalytical laboratory working to GLP and/or GCP regulations. There are a range of available automated systems and laboratory informatics that could be implemented and integrated to make an electronic laboratory. However, which are the appropriate ones to select and what is realistic and cost-effective for an individual laboratory? The answer is to develop an overall automation strategy that is updated periodically after each system or application has been implemented to assess if the strategy is still valid or needs to be changed. As many laboratory informatics applications have functional overlap or convergence, for example, Laboratory Information Management System, Electronic Laboratory Notebook, and Instrument and Chromatography Data Systems, the decision of which application performs a specific task needs to be carefully considered in the overall strategy. Ensuring data integrity and regulatory compliance, especially in light of a number of recent falsification cases, is a mandatory consideration for the overall strategy for an electronic bioanalytical laboratory submitting data to regulatory authorities.

R D McDowall

McDowall Consulting, 73 Murray Avenue, Bromley, Kent, BR1 3DJ, UK
Tel.: +44 20 8313 0934
E-mail: rdmcdowall@btconnect.com

There are many automated systems and **laboratory informatics** solutions that could be implemented in today's regulated bioanalytical laboratory for either GLP or GCP. The purpose of this article is to discuss the options available and to develop principles and strategies that can be used to design, implement and qualify and/or validate systems to produce an **electronic laboratory** environment that will ensure compliance with applicable regulations. Although this article is intended for regulated bioanalytical laboratories, un-bioanalytical laboratories that are unregulated can follow the principles described here as well and can make appropriate adjustments to their strategy if required. However, it should be understood that any data submitted to the US FDA, regardless of inclusion in GLP or GCP regulations, must comply with the requirements of 21 CFR 11 as stated in §11.1(b) [1].

The author has written about designing a paperless or electronic laboratory previously [2,3] but these articles discussed the electronic laboratory from a GMP perspective. Many of the principles for designing an electronic laboratory are common across GMP and GLP/GCP regulated laboratories, but this article will discuss the topic from the GLP and GCP perspective. In addition, the length of this article allows the author to discuss points in more detail than in the previous articles [2,3].

Some of the questions considered in this article are:

- Why work electronically?
- Can we use our existing paper-based process for electronic working?
- How does a laboratory actually work electronically?
- Do we have the necessary understanding to design an electronic laboratory?
- Do the available applications allow effective electronic working?
- How can we ensure the involvement of the users and the rest of the business in bioanalytical projects for the electronic laboratory?
- How can we ensure our electronic processes maintain the integrity of the data generated and derived from bioanalytical work?

This last point is important as this perspective article focuses on regulated bioanalytical laboratories that have to ensure **data integrity** and **regulatory compliance**. There have been a number of data falsification cases involving bioanalytical laboratories. One such case was that of Cetero, a CRO based in Houston (TX, USA), where a number of bioanalytical studies between 2005 and 2009 contained data that were falsified [4,5]. The FDA issued an untitled letter in July 2011 and cited the reasons for this as:

FUTURE SCIENCE part of fsg

Key Terms

Laboratory informatics: Software applications used in a laboratory environment.

Electronic laboratory: Laboratory where the working practices are largely electronic and paper output is minimal.

Data integrity: Procedures and mechanisms for ensuring that data remain intact and changes are authorized from the point of acquisition to the generation of a report. Integrity must also be maintained throughout the record retention period.

Regulatory compliance: Compliance with applicable regulations.

- The widespread falsification of dates and times in laboratory records for subject sample extractions;
- The apparent manipulation of equilibration or 'prep' run samples to meet predetermined acceptance criteria;
- The lack of documentation regarding equilibration or prep runs that prevented an adequate internal investigation to determine the extent and impact of these violations being conducted [6].

Therefore any electronic laboratory strategy needs to include provision for ensuring that all work is recorded within secure systems where users cannot access data via a hard drive except though an application. In addition, only authorized individuals can make modifications to data that are tracked by audit trails that cannot be accessed and changed by any user. These approaches reduce the opportunity and scope for data falsification.

This article should be read in conjunction with the articles in the *Bioanalysis* Special Focus Issue on 'Increasing productivity' [101,102], and the most pertinent of these articles will be referenced, where appropriate.

Why work electronically?

Paper, the only option available when the GLP regulations were first introduced, is a known medium that has worked well since then, so why not continue to work this way? To answer this question we need to consider the business and regulatory drivers that are dictating that laboratories need to work electronically if they do not do so now. The drivers for the electronic laboratory are twofold: regulatory and business. We shall consider each one in turn.

■ Regulatory drivers for the electronic laboratory

From the regulatory perspective, there are the following drivers for working electronically:

- Compliance with Electronic Records and Electronic Signatures final rule (21 CFR 11) [1]: The original request from the pharmaceutical industry was for a regulation to allow the use of electronic signatures to take advantage of technology. This regulation gives the legal basis for the use of electronic signatures in combination with the underlying US GLP regulation, 21 CFR 58 [7], but the issue is that in many laboratories the underlying process is still paper-based. With the publication of the Part 11 Scope and Application Guidance by the FDA [8], the regulatory pressure of 21 CFR 11 has abated somewhat. But electronic records must still be trustworthy, reliable and comply with the underlying predicate rule requirements (e.g., GLP or GCP);
- Avoiding hybrid systems: paper-driven processes means that hybrid systems predominate in the bioanalytical laboratory. A hybrid system (electronic records with signed paper printouts) is the worst possible situation, as two sets of records on two different media and their linkages have to be maintained. It is far easier to change to working with electronic media as there is just a single medium to deal with, therefore making records management easier;
- Compliance with other regulations and regulatory guidance: GLP regulations include computerized systems as either equipment or apparatus, which have to be fit for their intended uses [7,9,10]. This requires additional regulated guidance, such as the FDA's guidance for Computerised Systems in Clinical Investigations [11], the outdated Organisation for Economic Cooperation and Development publication on Application of GLP Principles to Computerised Systems [12] or the PIC/S document on Computerised Systems in GXP Environments [13] that is used by the EU for guidance when conducting GCP inspections [14]. Therefore, the validation and operation of computerized systems in regulated bioanalytical laboratories need to comply with these regulations and guidance. The author has previously published an article in *Bioanalysis* on computerized system validation [15] and is also the author of a book on the Validation of Chromatography Data Systems [16], so this topic will not be discussed further in this article;
- Interface with dossier preparation systems: all regulatory submissions (e.g., New Drug Application, Product License Application, Investigational New Drug or Clinical Trial Exemption are only allowed in electronic form now. Therefore, generating paper in the bioanalytical laboratory and then scanning the relevant pages into the submission is a waste of time and effort. Especially as the process needs to be validated and each page of each scan reviewed to see that it is correct;
- Ensuring data integrity: it is imperative that the integrity of any data be maintained from

the initial observation or generation of raw data/electronic record at the bench or the instrument through to the successive data transformations to the final results. It is better to use validated electronic mechanisms to do this than rely on hybrid systems and manual entry of data. This topic will be addressed in more detail later in this article;

- Automated regulatory compliance: including security and access controls, data file checksums and audit trail entries need to be considered when selecting and implementing systems in the electronic bioanalytical laboratory;
- Ensuring inspection readiness: regulated bioanalytical laboratories must be inspection ready, especially after the 2009 post inspection response program [17]. Now laboratories only have 15 working days to have a complete response to all the 483 observations made at the time of an inspection. Therefore, it is essential to be inspection-ready all the time. Validated applications and automated systems will help in this process rather than updating paper documentation prior to each and every inspection or corporate audit;
- Trending, checking and auditing electronic data: electronic data is easier to trend by taking the results of a search and transferring the data into software applications for analysis and trending. Audit trail data of study data can be reviewed to check that changes are authorized and justified by the person making each change, which is better than working on paper. Furthermore, electronic data is also easier and faster to audit and inspect if a suitably trained and experienced user is used to drive the software for the auditor or inspector. Risk-based approaches to data review; for example, review-by-exception (see below), can also be justified and applied, which are acceptable by regulatory inspectors.

Business drivers for the electronic laboratory

Although business drivers are presented second to regulatory drivers, the rationale for working using electronic workflows is probably a more important reason for change in laboratories where paper predominates. The main business drivers for change are:

- Standardized working practices: the design of common working practices, standard electronic templates and the verification of data entered into a system at the point of entry avoid individual ways of working. Verifying that the data are in the correct format or value means that the system does a first-pass QC check at entry rather than later in the process;
- Electronic working is faster than paper: electronic working means that the need to sign and date the paper output is replaced by automatic processes using validated systems. Here when a task such as creating, modifying and approving electronic records occurred it was recorded in the audit trails of the various applications used in the laboratory. This is contingent on the time stamp being correct (typically the network being linked to a reliable time source), the time zone is known [8] and that no typical laboratory user can change the time on a system via the operating system;
- Implementing review-by-exception: once data have been acquired and processed, the review by a second person can be sped up by using a technique known as review-by-exception. Here, the audit trail or an equivalent mechanism has identified where manual interpretation of data has occurred, data have been changed or there have been instrument failures that have required resolution by a user. Review-by-exception requires that any application supports this, the computerized system validation can demonstrate that changes are identified so that review-by-exception can be used effectively. As a result, the review of analytical data can be sped up by an order of magnitude, compared with a comparable paper or hybrid record review;
- Increasing laboratory capacity: capacity increases within a bioanalytical laboratory are required so that more work can be accomplished by the same or fewer staff, thus reducing the overall cost for analysis and interpretation per study;
- Increased speed of decision making: Analytical runs can be assessed against analytical criteria faster electronically than on paper. This is to determine if a run was acceptable or analytical method performance was consistent throughout a study;
- Data-sharing productivity: there is more efficient and faster sharing of electronic data

between the bioanalytical laboratory, PK, statisticians and QA staff than is possible with paper and hybrid records;

- Faster dossier preparation: dossier preparation and product licensing is faster electronically as there is no need to scan and check the resultant images.

The electronic laboratory: paperless or less paper?

Note the use of the word electronic, rather than paperless, that is used in the title and also throughout this article. This is deliberate. In many laboratories today there are huge amounts of paper printed, dated and signed, resulting in the painful fact that bioanalytical staff can spend as much time managing the paper output as performing the actual analysis. This is obviously not the best use of resources.

However, does electronic really mean no paper? The answer to this question is probably no, for cultural reasons as much as business reasons. For human reasons, we are used to working with paper so we need to change culture to be used to handling data electronically. Thus, the way that computerized systems help us to work electronically must also change. The business reasons that it may not be cost-effective to have everything electronic due to the low volume of work versus the cost of interfacing, validating and training staff to work electronically. Therefore, each building block, as we shall see when defining and executing the strategy for an electronic laboratory, must be cost justified to demonstrate its value to the laboratory.

Business processes in a bioanalytical laboratory

To gain an overview of the scope that an electronic bioanalytical laboratory encompasses, it is important to view this from several aspects. The first is the underlying processes within the laboratory that will be automated. It is important to realize that the foundation of the electronic bioanalytical laboratory is that business process must be designed for electronic working. An outline process flow for a typical bioanalytical laboratory is shown in Figure 1 and each part of the process is discussed briefly below. Some of the typical processes found in a bioanalytical laboratory are:

- Protocol management: defining and approving the protocol, protocol amendments and deviations, and reporting the study;
- Sample management: sample labeling, transport, receipt, storage, use (including freeze–thaw cycles) and sample disposal;
- Reagent and standard management: preparation, storage and use of reagents, management of analytical reference standards, preparation, storage and use of analytical standards, collection and storage of blank animal and human matrices for standards and QC samples together with their use and documented disposal;
- Method management: development and validation of robust bioanalytical methods for use by the laboratory. Confirmation of method performance prior to the analysis of samples from an individual study;
- Instrument management: documentation of instrument qualification, calibration, usage and maintenance work;
- Analysis management: analysis of samples from a specific study using qualified instruments, reagents and reference standard solutions and blank matrix. Identification of samples for reincurred sample reanalysis and the subsequent reanalysis;
- Data analysis, management and reporting: This occurs at two levels, the first is the storage and manipulation of the data files and electronic records generated by the analysis, and the subsequent interpretation and reduction to reportable results. The second is the records generated by the PK and statistical analysis of the subject plasma concentration versus time profiles or urine excretion amounts over time. These two phases of work can both be conducted in a bioanalytical laboratory or split between two departments.

Although all regulated laboratories work to the same regulations, each laboratory interprets these requirements differently. Therefore, this means that there can be differences in the detailed business processes from one laboratory to the next.

Can we use our existing paper-based process?

The simple answer to this question is a resounding no. The reason for this is to look at the basic processes and computerized systems: how they currently operate and how they integrate together. Although a laboratory can have the latest LC–MS instruments and data systems, in practice these can be islands of automation in

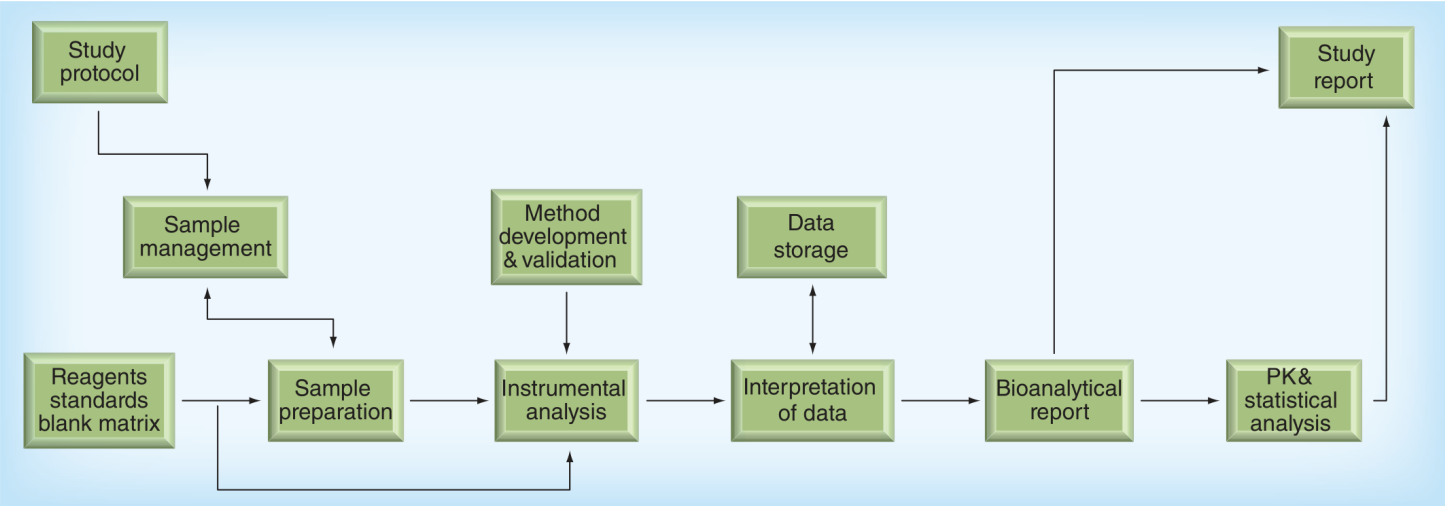


Figure 1. Outline process flow in a bioanalytical laboratory.

an ocean of paper. The main way that data are transferred from system to system is via manual input using paper or generating spreadsheet files as the transport medium. Furthermore, the process within a specific laboratory will have evolved over time and may have additional tasks that do not add any value to the laboratory output and it becomes very slow and inefficient.

■ Understanding & simplifying laboratory processes I

Before implementing any major computerized system, it is essential to map the current laboratory processes, understand them and then redesign them so that the application works electronically. The mapping includes the interfaces to other computerized systems and the associated data transfers. During this task of mapping the current business process, one objective is to identify any bottlenecks or delays in the workflow and understand the reasons for each one occurring. This is essential when transitioning from a paper-based process to an electronic one. The reason is that most laboratory processes are not designed but have evolved over time by the addition of new paper-based processes. Any system implementation should aim for a simplified and rapid electronic workflow rather than suffer with trying to automate an inefficient and paper-based process.

As stated above, the first stage in considering the electronic laboratory is to look at the basic processes and computerized systems: how do they currently operate and how do they integrate together, if at all. The scope of this work should start with the writing of study protocols and end with the study report, and can include a number of external departments such as research, toxicology, medicinal chemistry/pilot plant, clinical research, PK, statistics and QA, in addition to the bioanalytical laboratory.

An example of a portion of a current process is shown in Figure 2, this a sample management business process from a bioanalytical laboratory showing evolution over time. There are currently two formal process flows and one informal one, as follows:

- The first formal process is for internally generated samples. This is a simple process where samples arrive in the laboratory at an agreed time, prepared and assayed and then stored with a freezer log being updated;
- The second formal process is for externally generated samples. This procedure was developed following the loss of samples that were received but lost in the laboratory. The laboratory manager instigated this second process flow to prevent this from happening again. Within 24 h of the receipt of external samples they must be logged and checked against the inventory if one is available or an inventory prepared if there in none in the shipment. Then stored in a freezer, pending analysis;
- However, the third process is an informal and undocumented one. This was developed by one individual to streamline their work and is shown on the top right of the diagram (Figure 2). This was considered to be a simpler and easier way to work than the processes officially documented in the laboratory standard operating prodcedures (SOPs).

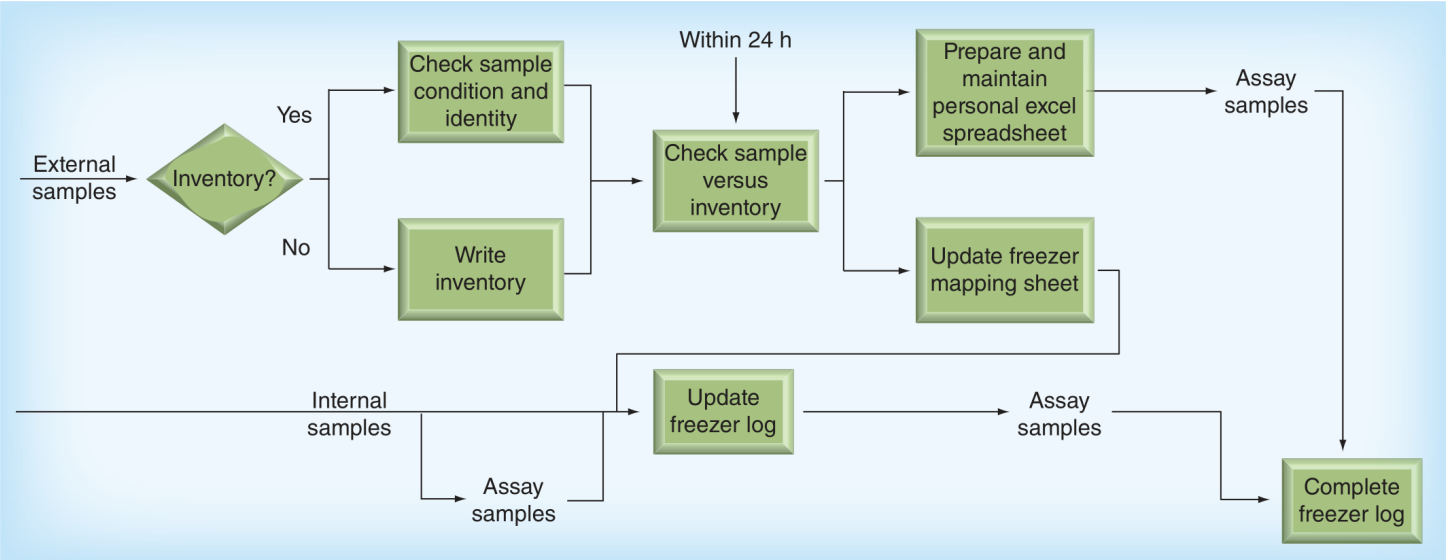


Figure 2. Current sample management process flows.

The problem if these three workflows were to be automated in either a Laboratory Information Management System (LIMS) or Electronic Laboratory Notebook (ELN) is that it requires three-times the work to specify, implement and validate. Why waste this effort for processes that are different and paper-based? It makes far more sense to redesign the way the laboratory works with a single electronic and all-encompassing sample management process. Hence the need to map and redesign, standardize, harmonize or optimize the processes in the laboratory. To achieve this we need to consider the three operating principles of an electronic laboratory, which are described in the next section of this article.

■ The operating principles of an electronic laboratory

When redesigning any process to work electronically, there are three basic operating principles of the electronic laboratory, which should be used to redesign or optimize the laboratory processes [18]. These are:

- Capture data at the point of origin: if you are going to work electronically, then data must be electronic from when it is first generated or observed. However, there are a wide range of data types that include observational data (e.g., hemolyzed sample), instrument data (e.g., pH, balance, LC–MS) and computer data (e.g., data files used for statistical or PK calculations using plasma concentration–time profiles). Interfacing systems and applications should be a major goal, but this has to be balanced with a cost-effective approach. For example, are the sample numbers and volumes sufficient to justify the cost and validation of interfacing?
- Eliminate transcription error checks: the second principle is to ensure that once data are captured electronically, they are never printed and re-entered manually into another computer system. All data transfers must be electronic, using validated processes with appropriate checks; for example, audit trails and checksums for file integrity to ensure that data are not corrupted. Ideally, only networked systems should be used to minimize data loss and for sharing data and information effectively. As a corollary to this principle, raw data must be defined as electronic records. Paper should only be a by-product of an electronic process, which is used for information only and is not defined as raw data. The electronic records produced in these workflows should be designated as records or raw data for archiving purposes;
- Know where the data will go: data storage repositories need to be designed for the electronic bioanalytical laboratory, which may be distributed across several applications, for example, LIMS, Instrument and Chromatography Data systems, or a Scientific Data Management System (SDMS), or simply secure network drives. To help size the storage, an estimate of the data volumes will be necessary. In addition, a predetermined plan of how data will be stored, for example,

by study number, drug project or product, and so on, must be developed before the repositories are implemented. This data storage plan will also include any file-naming conventions for data to ensure that an individual file, analytical run or study can be retrieved quickly and with the minimum of effort. To ensure no data loss in this electronic environment, it is essential that key hardware must be resilient and fault tolerant and that the backup and recovery processes must be robust and validated.

Implicitly required with this operating principle of the electronic laboratory is that standalone data systems are not adequate for data storage. Therefore, in the view of the author, all laboratory data must be stored on networked drives that have sufficient hardware resilience to prevent data loss from the failure of a single drive as an absolute minimum. In addition, rather than use file-based data systems, applications that use databases for acquiring and managing data as the audit trails are within the database rather than incorporated in the data file in contravention of 21 CFR 11 requirements for audit trails [1]. Backup strategies also need to be developed to ensure that data are not lost if a backup fails: consider differential rather than incremental backups or full backups that are executed each working day.

The key message when designing electronic workflows is to ensure that once data are acquired at the point of origin they are not printed out or transcribed again but transferred electronically between systems using validated routines. Paper is not to be used as the transfer mechanism and should only be printed when required; for example, audits, inspections and so on. Data storage must be networked and robust and, where necessary, thought must be given to file-naming conventions to identify data uniquely and be stored under projects or studies as appropriate.

Understanding & simplifying laboratory processes 2

Returning to the sample management process discussed earlier and illustrated in Figure 2, a process mapping workshop should help to identify and understand where there are bottlenecks and issues in the current process. The root causes of these bottlenecks will help a project team to challenge and improve processes using the three principles described in the last section. When the new process is redesigned the aims must be:

- To work electronically;
- To have effective and efficient transfers between both applications and organizational units.

Figure 3 shows the new sample management process implemented in conjunction with the introduction of a LIMS. Just by visual comparison of the old process shown in Figure 2 you can see that the new process is simpler and easier to understand. There is a single unified process in place of the two formal and one informal process under the old way of working. The process also uses computer-generated sample labels that have barcodes to enable better and more efficient sample tracking and management, however this is not shown in Figure 3, due to the detail required. Instead of three workflows in the current process, there is a single integrated workflow. Therefore, regardless of the source of the samples, they are all treated in the same way: allowing a unified SOP and LIMS implementation. The cost and time of redesigning the process can be offset against the gains from a simpler and cheaper LIMS implementation and validation, as well as cost savings in using the redesigned process.

The author's strong recommendation is that a laboratory should map and understand their workflows and processes. Before implementing any computerized system, processes should be redesigned to work electronically, thereby improving the speed and efficiency of the laboratory. To achieve this, it is vital that the applicable GXP regulations are understood and translated to the new processes, especially for electronic signatures under 21 CFR 11 and the applicable predicate rules as stated in the FDA Guidance on Part 11 [8].

Ensuring system resilience & preserving data in the new process

This article advocates working using electronic processes instead of ones based on paper. However, reliance on electronic workflows means that the laboratory needs to plan for how to handle common problems. If there are problems with the electronic process, the question must be raised, how can work continue? We will consider five common issues here:

- Hardware failure of a computer system: is there sufficient resilience in critical server components so that a system can cope with a single failure? Server hardware for critical applications must incorporate duplicate items to be resilient and fail-safe, for example,

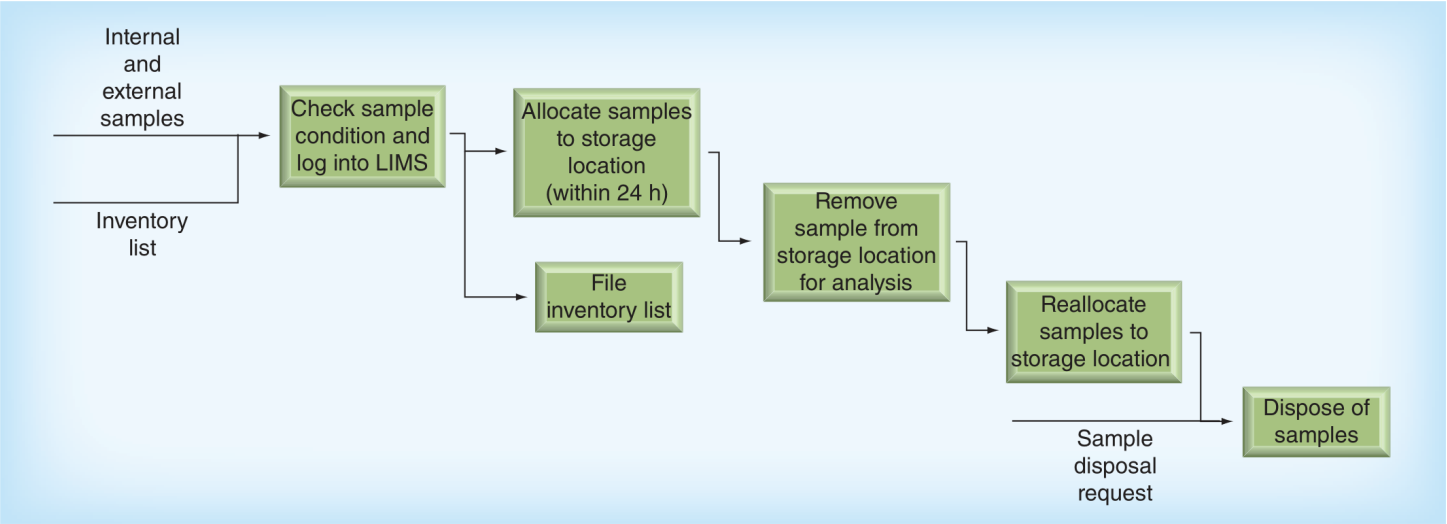


Figure 3. The optimized sample management process.
LIMS: Laboratory Information Management System.

duplicate power supplies, processors, disk controllers and data storage with 'Redundant array of inexpensive disks' technology. Redundant array of inexpensive disks or a separate storage area network, which both contain multiple disks, means that any data are duplicated across at least two disks in a way that if a single disk fails, then the data can be mathematically recovered. These hardware options should be used in conjunction with the backup and recovery software to limit the loss of data to perhaps a single file when a problem occurs. Ordinarily, if just a backup system is used, then data loss may be up to 24 h of data, however using hardware data resilience together with backup greatly reduces any potential data loss;

- Network failure: networks should have at least two different cable runs and associated communications equipment between buildings and floors so that the effects of network failures are minimized. This is especially important on larger sites where operations are spread across buildings; for example, the data center is in one building and bioanalytical laboratory facilities may be in one or more other buildings onsite. If using external hosting services that are certified to ISO 27001 [19] then the data center will have two separate data cables entering the site in different locations for communication resilience;

- Power failure: what happens if there is a power failure? Typically data centers have uninterruptible power supplies attached to prevent data loss from applications run across a network. The uninterruptible power supplies will have at least 5–10 min power before a generator starts to power the data centre. However, we also need to consider the impact of power failure in the bioanalytical laboratory and ask the question if can we accept the loss of the data from a single sample being analyzed at the time of the power failure?

- Application failure, for example, fatal software error: what happens to electronic data that was being acquired at the time one or more electronic systems failed due to a software error? If there is sufficient sample available for either reinjection or reanalysis this is inconvenient but acceptable. However, if the sample cannot be reassayed then the data will be lost and how will the laboratory cope with this? It may be that this is a low probability of occurrence but the main impact of this on a study needs to be considered;

- Contingency plans for nonavailability of systems: one question that often arises is should contingency plans be considered for alternative working if an electronic system is temporarily unavailable? Let us be realistic here, the answer is no. Delve into this topic in some more detail and ask the question, what viable options are there for manual LC–MS analysis? None. The same is true for a LIMS, it would be difficult to pick up a study when the information was in the unavailable system. Therefore the contingency plans need to be more realistic. Resilience in the computer

hardware and networks is essential and contingency planning needs to be centered around if there is a problem in the data center can analysis be continued locally? When the data center is available, data can be downloaded to the servers and work carries on as before.

Consideration of these issues and answering the questions proposed above, allows an organization to have a resilient approach to electronic data storage and management, which can be incorporated in the overall strategy for the electronic bioanalytical laboratory.

Automation & informatics tools

In this section, the review looks at the main building blocks that can comprise an electronic laboratory: the informatics applications and the automated instrument systems for liquid handling. This list is not exhaustive, but it provides an overview of what may be required for electronic processes within regulated bioanalytical laboratories. Other applications and systems may be used for individual laboratories to meet specific business requirements. The focus in this section is on systems and applications directly involved with the management and analysis of samples from bioanalytical studies. It does not consider general applications such as electronic document management systems and learning management systems that offer quality system support functions and will also be needed for complete automation of a bioanalytical laboratory.

There are a number of automation and informatics tools that can be used to construct an electronic laboratory and these are listed below and also in Table 1 together with the functions that they are capable of automating:

- Sample preparation/extraction automation [20–22];
- Instrument, calibration and maintenance management;
- Laboratory execution systems;
- ELNs [22–24];
- Method development and validation applications;
- Instrument and chromatography data systems;
- SDMS;
- LIMS;
- Statistical and PK analysis applications;
- Spreadsheet applications.

Note, in Table 1 there is overlap between some of the informatics tools that could be implemented in an electronic laboratory. There is functional convergence between some applications, for example, LC–MS data systems and a LIMS for the calculation of standard curves parameters and sample, QC and standard sample concentrations that could be performed by either system. Also, there is overlap between the functions automated by a laboratory execution system, which are more common in GMP QC laboratories and an ELN, which can be found in research as well as development and QC laboratories.

Spreadsheets are added to the list with a degree of hesitation by the author as normal use of them is not conducive to an electronic laboratory, since data input is manual and the system is considered a hybrid. As the overall objective is to design and implement an electronic laboratory, then a primary requirement of any system, or application is that it is not a hybrid system that is, hand-signed paper printouts linked to the electronic records generated by the system. This is the worst situation to be in and must be avoided at all costs as there are two sets of records to manage and co-ordinate with different media. Therefore, the only way that validated spreadsheets could be used within an electronic laboratory is if they operate within a secure and compliant environment, such as an SDMS or ELN, and that data input is performed automatically. Although there are software wrappers that provide spreadsheets with the 21 CFR 11 technical controls that are not present in the native worksheet (e.g., user-access privileges, audit trail and electronic signatures). However, the author discounts these as the spreadsheet is still used manually and this slows down a process as the data inputted still have to be checked for transcription errors. This check goes against one of the principles of the electronic laboratory, which is to eliminate transcription error checking.

Developing a strategy for an electronic laboratory

At this point, we have understood the business processes of the laboratory and optimized them for electronic working and know the automation and informatics tools that can be used. Now we need to bring them together to develop a strategy for the electronic laboratory. When designing an electronic laboratory, it is important to realize that this will not happen overnight and

Table 1. Automation and informatics tools that could be used to create an electronic laboratory.

Application	Main functions automated
Sample management	▪ Sample receipt and acknowledgement ▪ Sample storage locations ▪ Tracking freeze–thaw cycles of each sample ▪ Sample disposal
Sample preparation/extraction automation	▪ Dilution of samples ▪ Extraction and concentration of analytes from samples and standards ▪ Injection of sample for instrumental analysis
Laboratory execution systems	▪ Compliant execution of procedures (e.g., manual sample preparation) ▪ Preparation of standards and QC samples ▪ Data acquisition directly from pH meters and analytical balances ▪ Calculation of results from data acquired
Electronic laboratory notebooks	▪ Compliant execution of procedures (e.g., manual sample preparation, preparation of standards and QC samples) ▪ Compliant execution of spreadsheet calculations ▪ Data acquisition directly from pH meters and analytical balances ▪ Interpretation of integrated data and calculation of results
Method development and validation	▪ Devising and conducting experiments in method development (quality by design) ▪ Identifying critical factors in an LC–MS method for ruggedness and robustness evaluation ▪ Automating method validation experiments
Instrument and Chromatography Data Systems	▪ Analysis of samples ▪ Instrument control ▪ Data acquisition from instrument ▪ Integration of data ▪ Interpretation of integrated data and calculation of results
Scientific Data Management Systems	▪ Data management and storage ▪ Reading data files from different vendor's systems ▪ Conversion of data to archive format for long-term retention
Laboratory Information Management Systems	▪ Protocol management ▪ Sample management ▪ Reagent management ▪ Interpretation of integrated data and calculation of results ▪ Collation of results from the protocol ▪ Preparation of results tables for reporting or further data analysis
Statistical and PK analysis applications	▪ Calculation of PK parameters from study protocols ▪ Statistical analysis of results and preparation of report tables
Spreadsheet applications	▪ Automation of calculations ▪ Manual input of data ▪ Automatic input of data ▪ Hybrid system unless used within an scientific Data Management Systems or Electronic Laboratory Notebooks ▪ Can be used with Part 11 wrapper software

will take some time to implement. Therefore, it is important to have an overall automation strategy for the laboratory that is aligned with the overall business objectives of the organization. This strategy will need to be reviewed and revised on a regular basis, for example:

- Checking the alignment with the organization's business objectives, especially following reorganizations or mergers;
- Understanding how the electronic laboratory strategy will work if or when work is outsourced;
- Following the implementation of an individual system and its integration with the current operational ones;
- Introduction of new technologies and new applications or systems that may impact the overall direction of the laboratory strategy.

■ Strategic planning for the electronic laboratory

An overall strategy for the electronic laboratory needs to be generated by the laboratory, in conjunction with the external departments

involved with generating studies and using the results from them. The strategy should then be reviewed and approved by senior management. The strategy will contain the systems to be implemented and the order of implementation, together with an overall vision of where the laboratory should be when the process is completed.

This is illustrated in Figure 4, which also shows the dynamic nature of the planning process. The first laboratory strategy is formulated and two systems are implemented to move the laboratory to the vision outlined by Strategy 1. When the two system implementations have been completed, a review of the overall strategy, the current business objectives and available technologies/applications indicates that the strategy is updated, thus system 3 is implemented with Strategy 2 as the new target. This shows that the target is not stationary but moves with changes in the business, available systems and regulations: a dynamic and changing environment.

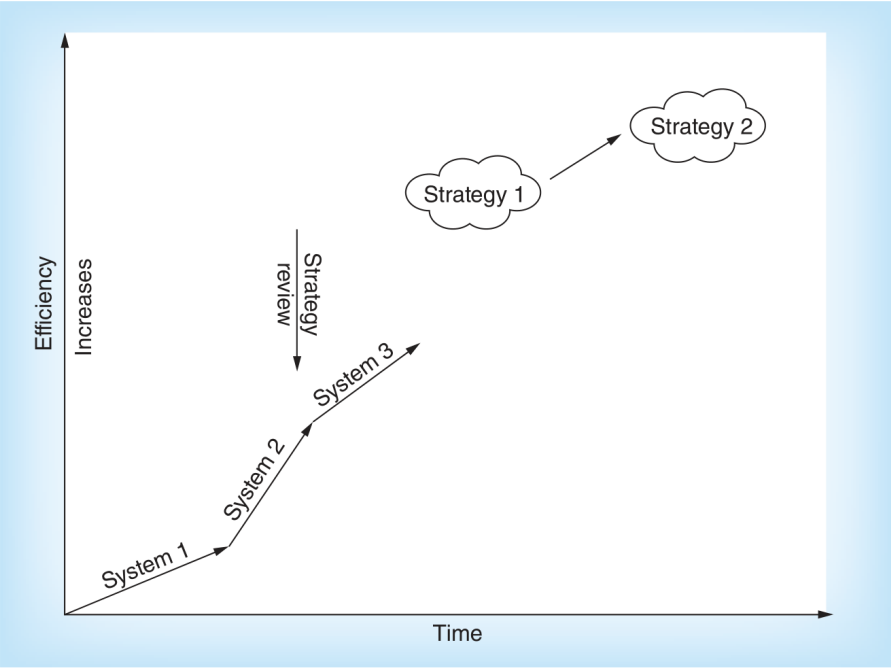


Figure 4. Strategic planning for the electronic laboratory.
Reproduced with permission from [3] © Scientific Computing/Advantage Business Media.

Systems & the operating principles of the electronic laboratory

Earlier in this review, the operating principles of the electronic laboratory were presented and discussed. These now need to be put into the context of the overall strategy and this is shown in Table 2 & Figure 5. The applications that could be involved to achieve one of the operating principles are shown in the second column of Table 2. It must be noted that the intent of this table is not to imply that all applications need to be purchased and implemented to achieve the operating principles of the electronic laboratory as this will depend on the strategy formulated by an individual organization. For example, one laboratory may determine that a network drive may be best suited as their data storage repository. In contrast to another that may require this function is best met by a scientific data management system as they have different instrument data systems and need a mechanism to read all data files in a central location.

In contrast, Figure 6 shows the general bioanalytical process flow, copied from Figure 1, with the different automation and computerized systems that can automate each task identified by each process activity. Again, this is not intended to imply that all applications and instruments must be implemented, as this will be determined by each laboratory in their strategy for their electronic laboratory. Equally well, alternatives to the applications and systems suggested here are acceptable provided that they meet a laboratory's business objectives and fit with the overall laboratory strategy.

Phased implementation of systems

If Figure 6 gives the impression of a jigsaw puzzle, this is deliberate as the overall strategy is equivalent to the picture of the completed puzzle that you find on the box top and the systems are the pieces of the puzzle. The question is how to assemble the pieces to complete the puzzle? There are a number of options that you could consider:

- Follow the process flow: identifying which functions would be automated by which system and defining the interfaces between systems and the data and information to be passed from one to another. The problem with this approach is that if a phased implementation is followed only portions of a system could be implemented at a time for example, sample management or protocol management and, in this case the system responsible for automating only a small a portion of the process would be unlikely to be cost-effective;
- The author's preferred approach is to take a layered approach. This differs to the point above, as a self-contained portion of the process can be automated and the benefits calculated for each area. This will be discussed now in more detail.

Table 2. Principles of the electronic laboratory and potential systems for their implementation.

Principle	Systems for the implementation of principle
Data capture at the point of origin	▪ Automated sample preparation instruments ▪ Instrument data systems (e.g., LC–MS and immunoassay) ▪ Electronic Laboratory Notebook ▪ Laboratory Execution System ▪ Laboratory Information Management System
Never transcribe data	▪ Laboratory Information Management System ▪ Electronic Laboratory Notebook ▪ Scientific Data Management System (managing data generated by the instrument data systems) ▪ PK analysis ▪ Statistical analysis ▪ Electronic document management system
Know where the data will go	▪ Laboratory Information Management System database ▪ Electronic Laboratory Notebook database ▪ Networked storage drive(s) ▪ Laboratory Information Management System database

In a typical laboratory, there will already be instrument data systems installed and it may be best to build outwards from this foundation, adding additional parts of the strategy until the overall strategy is completed. One element of the strategy may be to standardize on a specific data system, so when additional units are purchased, either for expansion or replacement, the qualification and validation costs are much reduced. In addition, the training costs associated with a new data system are minimized as the software application is known and understood by users in the laboratory. Therefore let us consider, as an example of the layered approach to system implementation, a bioanalytical laboratory with several instances of three different types of LC–MS data systems with a paper process for study and sample management, analysis and reporting. One version of an overall laboratory strategy envisions one type of data system for acquiring and processing LC–MS data and a LIMS to automate the study, sample and analysis management. To minimize risk and to provide a firm foundation for the overall strategy, the data

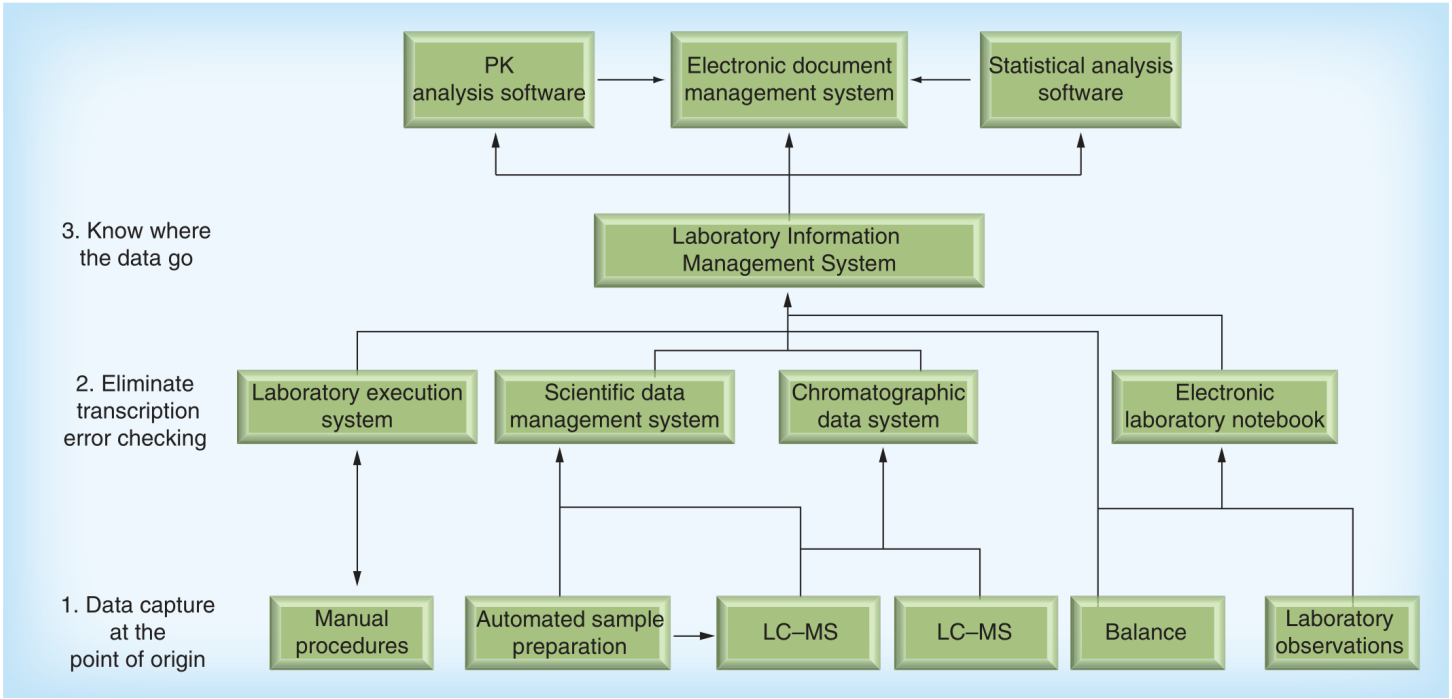


Figure 5. Electronic laboratory operating principles with potential applications to fulfill them.

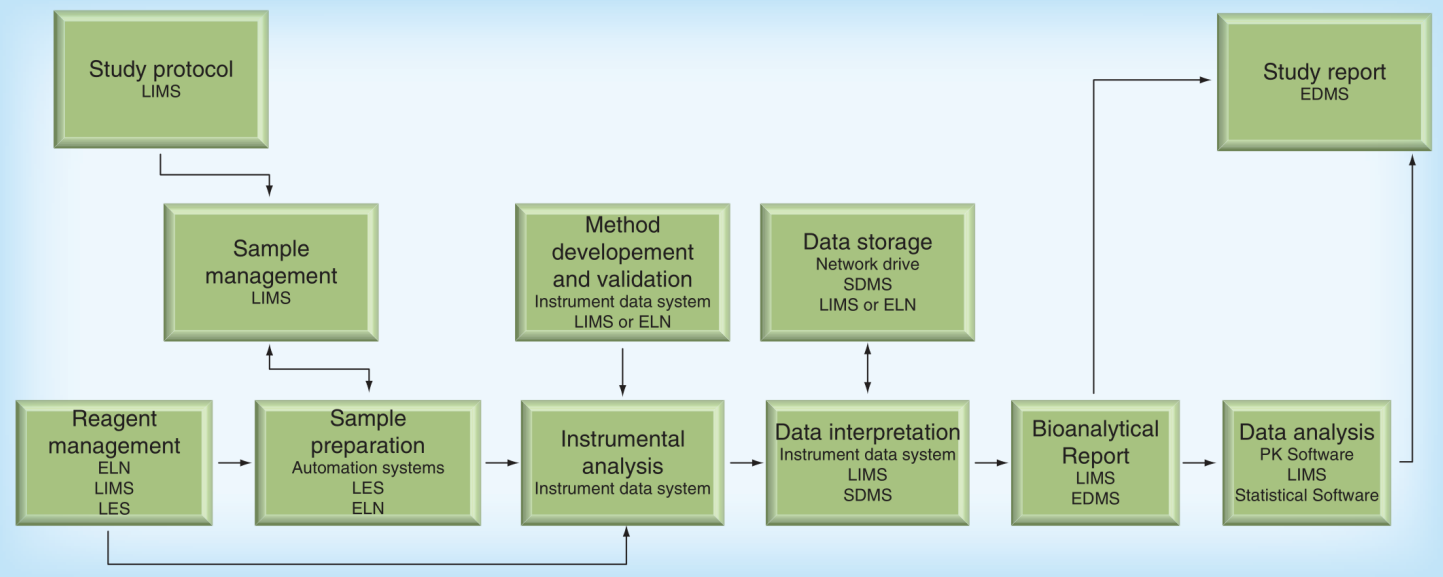


Figure 6. Bioanalytical process with potential systems for their automation.
EDMS: Electronic document management systems; ELN: Electronic Laboratory Notebook; LES: Laboratory Execution Systems; LIMS: Laboratory Information Management System; SDMS: Scientific Data Management System.

systems will be updated first and implemented first. Risk is minimized as the laboratory already has experience of working with various LC–MS data systems and the timeframe for implementation and validation is relatively short compared with a LIMS. In contrast, if the LIMS were implemented first, the lifecycle is longer and as the laboratory has little experience of working with a LIMS the project risk is increased. Therefore the new data systems can be implemented and validated. This approach has the advantage that there is now a single system and this makes training of staff easier, reduces validation costs and there is now just one data system application to interface to the LIMS at a later stage. There may be a transition period where the data systems perform the acquisition, integration and calculation of analyte concentration until the LIMS is implemented. Then the LIMS could take over the standard curve, QC and analyte concentration calculations, or if required the data system operations continue as before and only final calculated results are transferred to the LIMS.

When larger systems are considered, such as a LIMS, the scope of the system will likely extend outside of the bioanalytical laboratory and into surrounding business areas. One way of integrating these departments is to have trained users for input of study protocols or generating work lists and sample labels for taking samples from subjects. Information can be provided for taking the sample, for example blood, and centrifuging to obtain plasma for transfer to other labeled sample tubes. Where appropriate the system could warn a user to ensure low light levels if an analyte is photosensitive or to add preservative to prevent oxidation before analysis.

The tasks performed by the data system need to be defined as well as the interface and data transfer between it and other system and applications; for example, sample preparation systems, LIMS, ELN and/or SDMS. Some of the typical questions that may be asked during the preparation of a strategy may be:

- What is transferred from, say, a LIMS to the data system in terms of sample information, for example, order of samples or unique identity of a sample?
- What information is transferred from a sample preparation system to the data system, for example, sample volumes or dilutions used during sample preparation?
- Would sample identities and sample dilutions be transferred from the automated sample preparation system as an alternative way of working?
- Where would the standard curve and sample concentration calculations occur: on the data system or in a LIMS?
- How would clients and regulators review analysis records and study results?

Key Term

User involvement: Involvement of the laboratory staff and others in process improvement and implementation of the applications and automation systems in a regulated laboratory.

In the example above, the strategy may be extended to add automated sample preparation systems that can be interfaced with the existing LIMS and LC–MS systems. Data from the LIMS could be downloaded to the sample preparation systems to record the dilutions performed against sample identities. The sample identities and dilution factors for the batch can be transferred either to the LIMS or the LC–MS data systems to apply corrections to calculated results where appropriate. The sample preparation process is now automated and interfaced so that paperwork is reduced in the sample preparation, analysis and study management stages. Some areas still remain to be automated such as reference samples or instrument maintenance and calibration logs, which can be addressed in later phases of the strategy.

If a new type of application or system becomes available that has potential to be of benefit to a laboratory, it should be evaluated to determine if it is worthwhile of inclusion in the overall strategy. If this new type item is suitable, then the laboratory strategy should be revised to ensure that the of application fits well in the overall automation landscape. The revised strategy should be viewed and authorized by management to ensure their continued buy-in to the strategy.

Strategies look good on paper but they have to be turned into reality. Possible applications need to be understood at a detailed level to see if and how they fit with the redesigned process. As the application is understood in more detail, it may become apparent that the way it works is better and more efficient than the intended workflow. Therefore, the redesigned workflow should be modified and adapted to the application. Each application should be prototyped to ensure that the intended way of working is acceptable and meets the objectives of the automation strategy. Flexibility and confirmation of acceptability are essential in implementing any application or system to avoid making expensive mistakes.

As you can see, the electronic laboratory should be designed, not evolve by trial and error. It should be noted that one of the key principles in developing the automation strategy should be to limit the number of applications and systems wherever possible to obtain the maximum business benefit and reduce interface and validation costs.

■ Justification of individual systems

Within the overall scope of the strategy there will be a number of individual applications and systems that will be implemented and integrated to the electronic operation as listed in Table 1, the approach that should be taken for the overall strategy must be:

- There needs to be management buy-in for each application or system, or it will be difficult when decisions or resources are required for changing processes or system implementation;
- Each application or system must be self-justified from business and/or regulatory perspectives. This may include a cost–benefit analysis where the tangible and nontangible benefits are estimated versus the total cost of implementation and validation;
- Each application automates the portion of the analytical process efficiently;
- Each new application/system interfaces with existing systems to leverage bigger business benefits of the combined system. This is where a single system may be marginally cost-beneficial, but in combination with other systems becomes fully justified.

However, implementing steps towards an electronic laboratory requires the active involvement and co-operation of the analytical scientists, QA and laboratory management. An electronic laboratory will require changes, sometimes radical, in working practices not only within the laboratory but also outside of it. To achieve this, communication, effective management support and effective change management are required in the impacted areas.

Although project risk management is a key part of a laboratory automation strategy, there is not sufficient space to cover this topic in detail and the reader is referred to the review article written by the author [25].

■ Human factors in the electronic laboratory

User involvement in any electronic laboratory project is essential for the project to succeed. Therefore, this section looks at ways to involve users in a project and this starts with laboratory management. Management's role is to set expectations and goals for each project and allow the project team to work with delegated authority of the management. To help the project team further, management should ensure that performance objectives for successful roll-out of each system are included in the personal objectives of all laboratory personnel. On the other hand, the

absence of management support will cause the project to fail.

User involvement must begin from the start of each project, with inclusion of users on the project team. However for some projects, the user base could come from outside, as well as inside the laboratory, so bioanalysts and other departments should be represented in the project team membership. Their roles should be to ensure that user requirements are included in the new system.

Table 3 lists some of the factors for success and failure with automation and laboratory informatics projects. Two of the factors that could influence the outcome of a project to implement the electronic laboratory are:

- Long implementation times: a major cause of failure is a long project implementation time. Ideally, projects, especially those involving informatics such as LIMS or ELNs, need to have short implementation times of less than 1 year to ensure the focus and resources are maintained. An informatics project could be phased with core functions delivered with the first roll-out and additional features coming later;
- User training: training key personnel or super users on how to use the system is important to help the implementation and roll-out phases of a project. However, training of the user base is often reduced (train the trainer) or underestimated: it takes time for a user to understand and use a new system and this must be allowed for in the roll-out. Adequate training materials, SOPs and user guides must be in place, along with first-line help from super users to resolve problems. For larger systems, a suggestion is to offer refresher and advanced training to users between 3 and 6 months after the system has gone live.

For the electronic bioanalytical laboratory strategy to succeed it is important to understand the reasons for success and reinforce them. Equally important is to plan to avoid factors that cause projects to fail.

Ensuring data integrity

A key requirement of the GLP regulations [7,9,10] is the definition of raw data. In an electronic laboratory the raw data will be electronic as there will be little, if any printout of data. There is insufficient space to go into detail about what constitutes raw data in an electronic environment, so the reader if referred to a paper by the author on this subject for further reading [26]. However, the basic criteria for the integrity of raw data or electronic records are presented below and are derived from a document discussing the inspection of electronic source data by EMA inspectors [27]:

- Attributable: who acquired the data or performed an action and when? All activities and actions must be traceable to a trained individual;
- Legible: can you read the data and any associated entries?
- Contemporaneous: records and actions are documented at the time of the activity;
- Original: original record or observation or a certified true copy thereof;
- Accurate: no errors or editing without a documented audit trail of amendments;
- Complete: all data including any repeat or reanalysis performed on the sample and a subsequent data transformation plus the associated metadata and audit trail entries;
- Consistent: all elements of the analysis such as the sequence of events follow on and are date or time stamped in expected sequence;
- Enduring: not recorded on the back of envelopes, cigarette packets, post-it notes or the sleeves of a laboratory coat but electronically in the application or in a laboratory notebook;

Table 3. User involvement in electronic laboratory projects.

Factors for success	Factors for failure
▪ A worthwhile project, with business and laboratory benefits	▪ A sceptical approach
▪ Attention to detail in design	▪ No management or user involvement
▪ Analysis of the user's needs	▪ Replacing an existing system without adding new functions
▪ Thorough system testing	▪ Inadequate support or resources
▪ Thorough training of the users	▪ Not meeting user expectations
▪ Written objectives with predefined success criteria	▪ Inability or unwillingness to change ways of working
▪ Implementation of the core functions for large systems as a first phase	▪ Complex system design
	▪ Long implementation times

- Available: for review and audit or inspection over the retention period of the record.

Ensuring the integrity of data generated and derived during bioanalytical work is a mandatory requirement of the electronic laboratory strategy. The author has developed a list of ten compliance areas for data systems used in regulated laboratories that should be considered for ensuring data integrity [28]. Some of the main areas are discussed below.

Data integrity has a number of criteria, the first of which is to ensure the compliance of any application considered for inclusion in the strategy to the technical requirements of 21 CFR 11 [1]. Some of the considerations are:

- All users need to be allocated a unique user identity that is never shared or reused. In addition, passwords must only be used by their owners, there are many instances where passwords and user identities have been shared and this fails the 'attributable' criterion in the list above;

- Many data acquisition and sample preparation systems have file-based data storage meaning a user can access files via the operating system rather than via the application. This is unsatisfactory as it leaves a laboratory to demonstrate that the files cannot be changed after acquisition. Checksums within files are one answer but this should also be combined with direct data acquisition to a network drive as a minimum. This latter point also removes the need for the laboratory to backup the data acquisition systems as this will be performed more efficiently and effectively by the IT department;

- An alternative to file-based systems is to implement a SDMS, which places agents in specific directories on data-acquisition computers. When an analytical run is performed, any data files created are stored in these directories when an injection is finished. The SDMS agents poll the directory of specified time periods and transfer any new data files to the SDMS database where it can be tagged with predefined metadata to aid retrieval later. Polling time depends on how the data will be interpreted in next stages of the process, it can be as short as 1 min or as long at 12–24 h;

- An effective and encompassing audit trail is required in all applications. Although the FDA's Guidance on Part 11 [8] allows for alternative methods of ensuring data integrity other than an audit trail, the simple fact is that if a laboratory wants to work electronically in a networked environment then an audit trail for each application is mandatory. The problem with audit trails is that the information contained in the trail should be easy to understand and easy to search what has been changed. However, a better approach is to flag those records that have been changed after acquisition by users to allow review-by-exception;

- Electronic signatures need to be appended to the records that they relate and not simply noted in the audit trail. In addition, once the records are signed they must be locked, and noted by the system as locked and signed, but this is not always the case with many systems. Unlocking signed records for reinterpretation must require the approval of a senior analyst or manager.

Therefore, all data integrity criteria need to be considered as a key component of the overall electronic laboratory strategy.

Are the applications & systems ready for electronic working?

This area is a major obstacle for the electronic laboratory. The applications and automated instruments will perform their main task of automating a business process well, but the problems lie in the back-office portion of the processes that they automate. The functions lacking are the tasks that must occur but are not considered or well thought out, for example, second person review and QA review of work activities, data generated and interpreted, data integrity and audit trail events. These are lacking in the majority of applications used in bioanalysis. Even those packages that claim to have been specifically designed for the regulated laboratory and have the technical controls for electronic records and electronic signatures regulations are not able to demonstrate with evidence that a complete review of records has taken place. This needs to change.

Effective audit trails must identify that any unanticipated events have occurred, for example, correction of a value by a user. Such an action would require checking by a supervisor before approval of the batch run. In contrast, events that are expected in the normal operation of the process would not raise concern and should be marked as expected. If audit trails were implemented in this way, it would permit review-by-exception, resulting in a speedier assessment of the batch quality of an analytical run. In addition, there needs to be a functionality in the system

that records that a supervisor and a member of QA have both reviewed the data and the ability to record any findings for the analyst to correct. Although there are few systems that can do this, they are not pervasive throughout all bioanalytical software applications.

Critical success factors for the electronic laboratory

To ensure the success of building an electronic laboratory, there are a number of critical factors to consider that are listed in Table 4. The most important critical success factor is senior management support throughout the period taken to implement electronic laboratory, for the main reasons that budget and resources will only be released if the individual or individuals back the overall concept and see that successive system implementations and integrations are providing the anticipated business and regulatory benefits. Senior management also play a key role in minimizing resistance to the overall approach through direct persuasion of groups and individuals, as well as setting performance objectives for the implementation or use of specific automation and computerized systems.

Allied to senior management support is the leadership, encouragement and support of the management of the bioanalytical laboratory. The individual or the management team own the strategy document and need to review and revise it on a regular basis with input from all relevant parties. To ensure success of the strategy, the team needs to influence workers in the laboratory formally through the performance appraisal and objectives set for individual projects, but also informally through talking to individuals and teams.

QA is also important to involve in the overall strategy planning; as well as in design and implementation of systems that will aid and document review of study data. In doing this, regulatory inspections will also be facilitated. However, there needs to be training involved for QA staff, and also the applications are not always ready for complete electronic working yet, as discussed earlier in this article. In addition to QA, where systems also impact other departments that work with bioanalysis, they need to be involved in specifying the possible use of the systems in the strategy. Failure to involve external departments may result in some functions, or the whole system failing.

When redesigning the underlying processes in a laboratory, the approach should be evolution not revolution. A major reason is that in a regulated laboratory, the current workflows already comply with applicable regulations, therefore, any change has to comply with these regulations, which makes radical re-engineering difficult to accomplish. However, the revolution not evolution concept also impacts the whole user base. In changing from paper to electronic working practices, there will be major change over time and the management program must alter to ensure that users have the skills necessary to use the new systems and processes. If training is not sufficient, new staff with the required skills may be employed.

As discussed earlier, users can make or break any system and they need to be involved in all projects that impact them. Therefore, communication between the users, project teams and laboratory management is essential to help persuade people to change their ways of working. Part of this communication should include requesting input to specifications and evaluation of prototypes, as well as the formal testing of systems during the validation.

As systems do not implement themselves, a multidisciplinary project team will be necessary, which will be comprised of laboratory staff, QA, IT, other external departments and, where appropriate, vendor staff to ensure that the system is delivered as specified and within budget. Involvement of staff from other departments is important to ensure that all groups are involved in projects impacting those groups. It is also important that the project team members have the right mix of skills and have worked in a project team before. If this is not correct, the project team need to be trained to understand what a project is, how to work in a team and deliver a project.

One of the critical success factors for the electronic laboratory is organizational maturity to use new technology: how successful has the organization been implementing and using automation and IT applications? If the success rate is low, the approach should be to start on smaller projects, perhaps data acquisition or automation of sample preparation, rather than a big informatics project. Learn from the project and apply the principles to bigger ones. This approach is to ensure that the overall strategy is capable of completion, rather than sinking with the first project.

The last critical success factor to discuss is maintaining current work commitments. It will be inevitable that projects will take highly qualified staff away from their normal duties. Therefore, it is imperative that laboratory management plan how the studies in progress and being planned will be delivered as promised. This may be to use contract laboratories or engage temporary staff to backfill those bioanalysts working on projects.

Table 4. The main critical success factors for implementation of an electronic laboratory.

Critical success factor	Issues to consider for success
Senior management support	Provide a clear vision of where laboratory is going with periodic revisions Budget support over 3–5 years (Later) track record of cost-effective application implementations Frequent liaison and feedback Support of each project initiative in public and in private
Involvement of laboratory management	Initial assessment of laboratory processes and use of existing IT solutions Develop initial strategy for the electronic laboratory with phased implementation Review and revise strategy on periodic (annual?) basis Incorporate learning points from previous implementations into forward plans
QA involvement in projects	Design and implementation of systems that facilitate and document QA review of study data (and hence regulatory inspections) Training to review study data electronically
Involve external departments and organizations	Who is used in generating samples for the laboratory? Who uses the information generated by the laboratory? All need to be involved in designing the strategy and also when specific applications are being designed and implemented
Evolution not revolution	Build on the current strengths and ways of working in the laboratory Change the laboratory incrementally with every application
Change management program	The current skill set at the start of the strategy may not be what is required in the paperless laboratory Assess the skills and acquire or retrain staff with required skills Many people do not like change; the program will need to explain the new processes and ways of working and encourage staff to use them
User support	Systems will not operate on their own and will need laboratory staff to use them A communication program is essential to persuade people to change their ways of working Identify and train super users to help implement system and help to drive adoption of a system Identify and train product champions who have a goal to get adoption of a specific system Solicit and use offers of help Request input into the systems design Demonstrate prototype systems for user feedback
Financial justification	Each application must be justified individually Include incremental IT improvement where necessary (e.g., network capacity) Leverage benefits from existing applications where appropriate
Proactive management of project risk	Projects in the strategy will have common risks and individual risks that will need to be managed to ensure that the project is delivered successfully See paper on project risk management [25]
Organizational maturity to use technology	How is IT used in the organization? How successful is the organization in implementing IT systems? Assess current maturity to use electronic workflow?
Project resources available with correct skill mix	Analytical staff will be needed for working on the applications but will be in competition with the normal work Staff must be dedicated to the project (include changing position descriptions) Some staff may need to be retrained with skills for implementing computer applications
Multidisciplinary project teams	Involvement of IT, QA and vendors in the projects that make up the overall strategy is key
Maintaining current work commitments	Laboratory must maintain commitments to the organization while implementing applications Consider use of temporary staff or contract laboratories to ensure that work is still delivered on time

QA: Quality assurance.
Reproduced with permission from [3] *© Scientific Computing/Advantage Business Media.*

If staff time is split 50:50 between normal and project work, this needs to be handled carefully, as when a work deadline calls, the project may suffer. This calls for careful management and planning of how to handle these situations.

Knowing the critical success factors of the automation and informatics projects that comprise the electronic laboratory strategy is important as it allows laboratory management and project team leaders to plan for success.

Conclusion

This article has discussed a mechanism of implementing an electronic bioanalytical laboratory from understanding and optimizing existing business processes or workflows in the laboratory to utilize efficient and effective electronic working practices. In doing this, there is an implicit move from paper to electronic raw data. The systems and instruments that could be used to build an electronic laboratory have been discussed and these are used to develop an overall strategy for the laboratory as a single system cannot provide all of the functions. Finally, the critical success factors for an effective implementation of an electronic laboratory are presented. One problem exists for an electronic laboratory: the applications are not available that record an electronic QA review. The focus of the majority of systems is on the functional delivery (e.g., automation of a process); however, it is just as important to ensure that the second person review is documented as well; in many systems this review is not documented effectively.

Future perspective

There are current applications that can be used to construct an electronic laboratory, however they are not perfect. The main functions work efficiently for the acquisition data, transformation into results and the ability to generate reports. However, the regulatory compliance of these in an electronic workflow is lacking in the majority of the applications. While applications have security and audit trails, they are passive rather than active in terms of helping a second person review. What is required is that the audit trail is integrated throughout the data workflow and, at this level, has a simple traffic light function. Green is equivalent to no changes, all data conversion was performed to predetermined routines, and no human changes have occurred. Red is where data have been changed or been deleted. Within a bioanalytical laboratory, users will be more used to working electronically, but there will be the same pressures from senior management to get an application working yesterday; an attitude that must change. In the future, if a bioanalytical laboratory is not working electronically it will not survive in a global market.

Financial & competing interests disclosure

The author has no relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript. This includes employment, consultancies, honoraria, stock ownership or options, expert testimony, grants or patents received or pending, or royalties.

No writing assistance was utilized in the production of this manuscript.

Executive summary

- This perspective article looks at developing a strategy for a regulated electronic bioanalytical laboratory based on the business and regulatory drivers impacting the pharmaceutical industry.
- Business processes in a bioanalytical laboratory must be mapped and optimized for electronic working before implementing any informatics solutions. The basic principles of an electronic laboratory are that data are captured at their point of origin, there is no retyping of any data and you must know where the data will be stored.
- A strategy for a laboratory should be developed. This starts with understanding the informatics tools that could be used and mapping them to the optimized business process. Many applications have overlapping or similar functions, decisions should be made which function will be carried out by which application and incorporated in the strategy document.
- Applications should be justified on their own merits and when interfaced with existing informatics solutions already implemented. The strategy should also be reviewed and updated regularly.
- This perspective article concludes with discussion of the critical success factors for successfully implementing an electronic environment in a regulated bioanalytical laboratory.

References

1 US Food and Drug Administration. Electronic Records; Electronic Signatures final rule, 21 CFR 11 1997.

2 McDowall RD. Designing a paperless laboratory. *Am. Pharm. Rev.* 3(4) 12–15 (2004).

3 McDowall RD. *Designing a Paperless Laboratory.* Scientific Computing and Instrumentation, Advantage Business media. NJ, USA, L8, L10, L12 and L14, (2005).

4 US FDA. Cetero Laboratories, 483 Observations, May 2010. www.fda.gov/warningletters

5 US FDA. Cetero Laboratorie,s 483 Observations, December 2010. www.fda.gov/warningletters

6 US FDA. Untitled Letter to Cetero Laboratories, 26 July 2011. www.fda.gov/warningletters

7 US FDA. Good Laboratory Practice for Non-Clinical Studies, 21 CFR 58 (1978). www.fda.gov

8 US FDA. Guidance for Industry Part 11 Scope and Application (2003). www.fda.gov

9 Organisation for Economic Cooperation and Development. *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring Number 1. OECD Principles of Good Laboratory Practice (As Revised in 1997).* Organisation for Economic Cooperation and Development, Paris, France (1998).

10 WHO. *Good Laboratory Practice (GLP), Quality Practices for Regulated Non-Clinical Research and Development.* WHO, Geneva, Switzerland (2009).

11 US FDA, US Department of Health and Human Services, Center for Biologic Evaluation and Research *et al. Guidance for Industry, Computerised Systems Used in Clinical Investigations.* FDA, Silver Spring, MD, USA (2007).

12 Organisation for Economic Cooperation and Development. *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, Number 10. GLP Consensus Document, Principles of Good Laboratory Practice for Computerised Systems.* Organisation for Economic Cooperation and Development, Paris, France (1995).

13 PIC/S Secretariat. *Pharmaceutical Inspection Convention/Pharmaceutical Inspection Co-operation Scheme. Good Practices for Computerised Systems in regulated 'GXP' Environments.* PIC/S Secretariat, Geneva, Switzerland (2007).

14 EMEA. Annex III: To Procedure For Conducting GCP Inspections Requested By The EMEA: Computer Systems EMEA/INS/GCP/444656/2007 Procedure no: INS/GCP/3/III-Rev 1 (2007). www.emea.europa.eu/docs/en_GB/document_library/Regulatory_and_procedural_guideline/2009/10/WC500004468.pdf

15 McDowall RD. Cost-effective and business-beneficial computer validation for bioanalytical laboratories. *Bioanalysis* 3(13), 1487–1499 (2011).

16 McDowall RD. *Validation of Chromatographic Data Systems, Meeting Business and Regulatory Requirements.* Royal Society of Chemistry, Cambridge, UK (2005).

17 US FDA. Post inspection response program. In: *Federal Register.* 74, 40211–40212 (2009).

18 Jenkins S. Presented at: *The Pittsburgh Conference on Analytical Chemistry and Applied Spectroscopy.* Chicago, IL, USA, 7–12 March 2004. www.scientificcomputing.com/articles/2011/05/ensuring-data-integrity-regulated-environment#.UqeCq8lFDIU

19 International Standards Organisation. *ISO 27001: 2013 Information technology. Security techniques. Information security management systems. Requirements.* International Standards Organisation, Geneva, Switzerland (2013).

20 Meadows K, Oliver M, Liddicoat T. Comparison of sample preparation approaches for bioanalytical workflows and their affect on productivity. *Bioanalysis* 5(14), 1729–1733 (2013).

21 Patel V, Leach D, Hornberger M *et al.* Automating bioanalytical sample analysis through enhanced system integration. *Bioanalysis* 5(13), 1649–1659 (2013).

22 Pearsall AB. Implementation and challenges of electronic notebooks. *Bioanalysis* 5(13), 1609–1611 (2013).

23 Schoup RE, Beato BD, Pisek A *et al.* Implementation of an electronic laboratory notebook to accelerate data review in bioanalysis. *Bioanalysis* 5(13), 1677–1689 (2013).

24 Rubacha M, Rattan AK, Hosselet SC. A review of electronic laboratory notebooks available in the market today. *J. Lab. Autom.* 16(1), 90–98 (2011).

25 McDowall RD. Risk management for laboratory automation projects. *J. Lab. Autom.* 9, 72–86 (2004).

26 McDowall RD. How raw are your data – 2012? *LCGC Eur.* 25(2), 88–107 (2012).

27 GCP Inspectors Working Group. *Reflection Paper on Expectations for Electronic Source Data and Data Transcribed to Electronic Data Collection Tools in Clinical Trials.* European Medicines Agency, London, UK (2010).

28 McDowall RD. Ensuring data integrity in a regulated environment: 10 essential chromatography data system compliance areas. *Scientific Computing* March/April 2011.

Websites

101 Increasing Productivity – Special Focus. *Bioanalysis* 5(13), (2013). www.future-science.com/toc/bio/5/13

102 Increasing Productivity – Special Focus. *Bioanalysis* 5(14), (2013). www.future-science.com/toc/bio/5/14

Today's Challenge in Cybersecurity

Defending Against Ransomware

October 6, 2021

Presentation Notes

Full presentation available at AlturasAnalytics.com

Bo Cheng, Ph.D.
Director of Information Technology
Alturas Analytics, Inc.

Alturas Analytics, Inc.
The LC-MS Experts

Session Description and Objectives

- Review the heightened ransomware attacks in recent years, analyze how ransomware works and the damages it can cause to the corporate.
- Raise awareness of ransomware for corporate leadership and ordinary employees.
- Planning by the corporate management and best practices for ordinary employees to mitigate the risk.
- Recommend actions the IT Department can take to combat the ransomware attacks.

Ransomware Surge Since 2020

- Recent High profile victims in US:
    - Garmin - July 2020
    - CNA Financial - March 2021
    - Applus Technologies - March 2021
    - Quanta Computer - April 2021
    - ExaGrid - May 2021
    - Colonial Pipeline - May 2021
    - JBS Meatpacking- May 2021
    - Kaseya (Irish with US headquarters) - July 2021

- Globally there are 740 named victims in 02 2021 alone
- 148% increase in ransomware attacks since the pandemic (sources: Forbes)
- The surge is probably due to a confluence of factors:
    - Popularity of anonymous payment (Bitcoin)
    - Hasty retooling of infrastructure to accommodate WFH by IT during the pandemic
    - Maturing of ransomware ecosystem (ransomware for hire market)
    - Recent tensions in geopolitics

What is Ransomware?

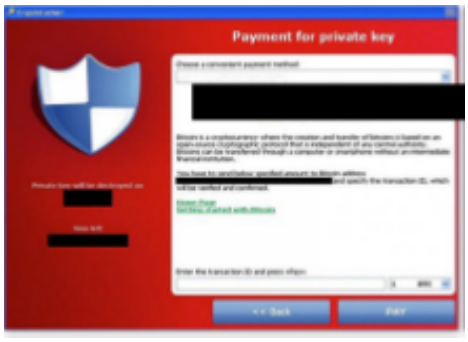
- Infiltration of malware into corporate network.
- The malware encrypts files it can access across the entire network, including hot backups.
- Business ceases to operate due to inaccessibility of encrypted files.
- Threat actor demands payment for decrypting.
- Increasingly, in some cases, confidential information is exfiltrated. Threat actor threatens to make it for public view if not paid.

Ransomware = Malware + Cryptography

For practical purpose, the victims cannot decrypt the files w/o the key from the threat actor.

History

Although Internet extortion could be traced back to late 1980's, ransomware did not become popular until the arrival of anonymous payment (Bitcoin). The first notable ransomware was Cryptolocker in 2013 - it targeted individuals and asked $300 in exchange for the key.



Today's Ransomware

- Targets businesses, asking for millions of dollars
- Has become an ecosystem on dark web
- RaaS (Ransomware as a Service) for hire, like "Killer for Hire"

The Damages

- Ransom payment: Usually several million USD, in form of Bitcoin. About 70% of victims choose to pay
- Interruption: Usually a week or more even if you pay the ransom. For most victims it took several weeks to come back to normal operation
- Cost in forensic investigation, damage assessment and control
- Legal ramifications if customer data is exfiltrated, possible restitution
- Regulatory compliance: Data breach issues - HIPAA, GDPR, CCPA and many more
- Reputation damage and loss of clients, contracts and revenue: Having the company in such news headline alone is damaging enough

Ways of Malware Infiltration

Primary Way: Through User Interactions

- Clicking links in malicious emails
- Opening attachments in malicious emails
- Visiting malicious websites
- Downloading malicious contents
- Leaking credentials (passwords) accidentally or by malicious insiders
    - 91 % Cyberattacks Start with Phishing Emails (sources: PhishMe/Cofense)
- System Vulnerability Exploitation
    - Vulnerabilities in Exchange Server (Hafnium attack) eventually turned to ransomware in March and April 2021 - many victims
    - SMBv1 EternalBlue vulnerability and WannaCry of 2017
- Weak Information Security Policy
    - Allowing weak or shared password
    - Giving users more privileges than they need
    - Not giving users clear guidance
    - Some small businesses may not have an Information Security Policy at all
- Security Misconfigurations by IT

Counter Measures

At Corporate Leadership Level

- Get Top Management Involved
    - Cybersecurity has evolved to a business issue, no longer a simple technical issue
- Foster a Cybersecurity-aware Culture
    - Cybersecurity is the responsibility of each employee, not just the IT Department
- Give IT Department Sufficient Resources
    - Money and manpower so it can act proactively
- Consider Cybersecurity Insurance
    - Especially important for small businesses to remain financially solvent if attacked
    - Be aware of the coverage. Does it cover 3rd party (customers) IP loss?
- PR Readiness
    - When compromised if there is no corporate response or announcement, it creates confusion and worry for customers and causes further reputation damage

At IT Department Level

- Periodic User Awareness Training
    - This is the #1 counter measure. No technical measure can offer 100% protection
- Conduct periodic phishing email exercise for all employees
- Tag external emails
    - Remind users such emails are potentially harmful
    - Promote zero-trust email security policy
- Prohibit personal use of work email
- Actively discover system vulnerabilities and patch timely
    - Following vendors advisories and tech news
- Establish and enforce Information Security Policy
    - Access policies based on "Need to Know" and "Least Privilege" principles
    - Robust password policies
    - Multi factor authentication
- Reduce attack surface by reducing exposure on the Internet
    - Placing servers behind firewall/VPN if possible
- Monitor security events and logs
    - SIEM (Security Information and Event Management) SIEM can be quite "noisy"

- Establish and Maintain
    - Firewall rules allowing utilized traffic only
    - Web filter to block malicious sites
    - Anti-virus at multiple places (emails, firewall and endpoints)
- Conduct Periodic Penetration Tests
- Maintain a DMZ (Demilitarized Zone)
    - Placing high risk servers in DMZ
- Maintain Robust Cold Backups
    - Off-line backups that malware cannot reach
- Partition storage servers
    - Assign permissions per "need to know" principle to limit the damage
- Have a contingency plan and mock test it

At Ordinary Employee Level

- Follow Information Security Policy
- Check with IT for emails from untrusted sources you are not sure of legitimacy
- Don't open email attachments out of curiosity
- Hover mouse to reveal the linked address in email web links before clicking
- Utilized "Preview'' feature in Outlook before fully opening attachments
- Report your computer's suspicious behaviors
- Visit work related websites only
- Never click "Clickbait"
- Safeguard your passwords

Best Way to Combat Ransomware:
Prevention, Prevention and Prevention!

The prevention of ransomware involves entire company and heavily relies on ordinary employees' daily activities at their workstations. No technical measures taken by IT will provide 100% protection.

Contact Information:
Bo Cheng, Ph.D.
Director of Information Technology
bcheng@alturasanalytics.com

Alturas Analytics, Inc.
1324 Alturas Drive
Moscow, ID 83843

Alturas Analytics, Inc.
The LC-MS Experts
www.alturasanalytics.com

Bioanalysis ZONE

Contact us

Editorial Department

Editor-in-Chief
Naamah Maundrell
n.maundrell@bioanalysis-zone.com

Business Development and Support

Head of Advertising
Dionne Murray
d.murray@future-science-group.com

This supplement is brought to you by Bioanalysis Zone in association with:

Alturas Analytics, Inc.
The LC-MS Experts