Energy Credit Best Practices

Chapter Excerpt Addressing

Information Technology

First Published Version, October, 2022

Table of Contents

ACKNOWLEDGEMENTS

White papers issued by the CCRO are the product of the efforts of its community of members. The views expressed in any particular CCRO paper are attributable only to the CCRO itself and do not necessarily represent the views or intentions of an individual member.
Preparation of our papers primarily involve a subset of CCRO members that possess a keen interest in the subject topic. This "working group" then designs, does the research, and authors the paper. Certain external parties may also assist on an ad hoc basis. The efforts of all these parties are greatly appreciated. While this group continues with its work on subsequent chapters, all interested parties are encouraged to contact us at info@ccro.org .
The CCRO extends special thanks to the following organizations and individuals who continue to dedicate valuable time, resources, and expertise to this working group which is dedicated to publishing *Energy Credit Best Practices*.

Working Group Leadership Team

Scott Davis (Project Manager) Judson Park Energy		Nithya Venkatesan (Co-chair), Navitas Assurance	
Roderick Austin (Coordinator) Cube Logic		Tom Birmingham, Emera	
James Goerig One Source Risk Mgt		David Klein Analysts International	
Craig Enochs Reed Smith		Mike Burger Veritas Total Solutions	

Content Editors

Steve Brown Mansfield Energy		Ken Robinson Engie	
Phil Roan Motiva		Chris Jackson Allianz Trade	
Mike DeLuca One Source Risk Mgt		Ying Hall, Tacoma Power	
Miguel Correa, Motiva		Kevin Kindall Hartree Partners	
Grant Carter Vistra Energy		Glen Mackey, Former CRO at NRG	
Bjornar Eide Mid-Del Consulting		Pat McKinnon Navitas Assurance Partners	

1. Introduction

1.1 Our Objectives

This is just one chapter in our on-going work towards a comprehensive CCRO white paper that documents best practices to be found in the energy Credit Risk Process. We intend for this work product to be subject to an annual peer-review and updated to always reflect the latest industry developments.

A recurring thread throughout the entire paper, and one notably demonstrated in this chapter, is the interdependence between Credit Risk and many other functions within an organization. In this chapter, we hope to strengthen the Credit Risk function's ability to leverage technology to work with other company functions more effectively. Working together is becoming more critical today as interdependence and associated information flows are rapidly growing

The use of Information Technology (IT) to support all aspects of business continues to increase at an ever-accelerating rate. This phenomenon is having a significant impact on data-oriented professionals, such as energy Credit Risk Managers. From simulating future exposures to collateral management, credit risk professionals have become increasingly reliant on technology to succeed at managing the credit risks created by their company's businesses.

The ability of IT to improve the credit risk function's capabilities and efficiencies is undeniable and will continue to advance as Digitalization progresses at energy companies. At the same time, credit risk managers need to be aware that this reliance on technology can be a double-edged sword if not prudently managed.

The CCRO advocates here a set of best practices that will yield specific benefits:

- Leverage technology to improve effectiveness and efficiency of energy Credit Risk operations
- Diminish the risks that rapid change may pose to the entire Credit Information Ecosystem.

The direct responsibility for accomplishing these two goals falls squarely on both the energy Credit Risk professionals and the IT professionals supporting the company's credit function.

This chapter provides specific recommendations for the best practice use of information technology in support of credit operations. Discussion around each recommendation provides background and context for the risk professional to better understand them and to assess any gaps that might exist in current practices.

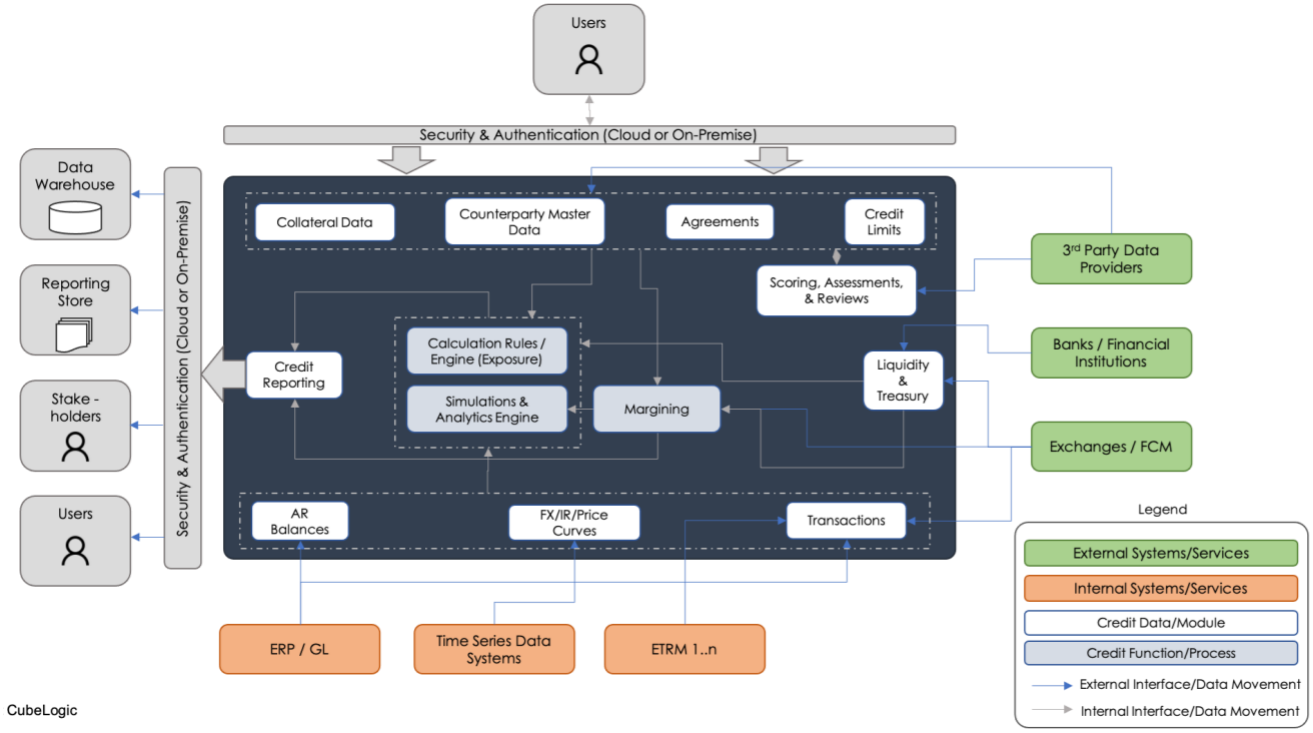
- We suggest that a formal benchmarking initiative of current technology practices versus those recommended herein could greatly facilitate a company's prioritization of internal change initiatives and help build management support for implementation.

1.2 This Chapter's Scope: The Credit Information Ecosystem

The Digitization of the credit process requires data from disparate sources from both inside and outside the organization. These sources can include a complex network of Systems and services, data, software applications, and processes. This paper refers to this amalgamation of credit data and processes as the Credit Information Ecosystem. Figure 2 below provides a visual example of what an illustrative Credit Information Ecosystem may look like.

Of course, this will vary for every organization, but the basic concept is apposite. This network can engage multiple users and stakeholders, including IT and credit personnel, third-party data providers, banks, and financial institutions. It requires Security and authentication interfaces, data warehousing and reporting stores. It entails interfaces with enterprise resource planning (ERP) systems, General Ledgers (GLs), Energy Trading and Risk Management (ETRM) systems, and time-series data systems. This Ecosystem also supports critical exposure, analytic and margining calculations, which facilitate key credit-related decision-making, including credit limits and collateral management.

Figure 1: Credit Information Ecosystem & Data Flow *Source: Cube Logic*



1.3 Industry's Move Towards Digitalization

We find that most sectors of the energy industry are today moving towards "digitalization" of their credit risk operations along with the operations of many other functions.

"Digitalization" - The use of digital technologies to change a business model and provide new revenue and value-producing opportunities. Refers to moving away from manual processes towards more automated and systematic processes.

This chapter accommodates this clear trend, and even helps credit professionals to capture the greatest benefits from digitalization. Our emphasis here for the credit professional is to better understand what advancements should be taking place within a Credit Information Ecosystem as the credit functions inevitably migrate to a more digital environment.

1.4 Core Themes of this Chapter

There are six themes in this chapter which are at the core of improving a company's Credit Risk operations and ensuring an effective Credit Information Ecosystem. Our hope is that these principles will provide understanding to credit professionals of what should be expected from technology to improve the management of their credit portfolio in today's increasing IT-centric environment.

While the CCRO recognizes that every company is unique, we hold that these core principles and the related best practices discussed further below apply to all energy credit managers and their respective Credit Information Ecosystems.

Following are the central themes found throughout this paper, which the CCRO believes an energy company must strive to establish in their credit operations Emphasis for the credit professional here is to understand what factors should be taking place within a Credit Information Ecosystem as the credit functions inevitably migrate to a digital environment.

1.4.1 Alignment

IT strategies, including the overall IT strategy of the organization, should align with the Credit Group's evolving needs in pursuit of more effective credit operations and execution of their fiduciary responsibilities.

It is difficult to over-emphasize the importance of the orientation of the Credit Group's operational objectives to the company's enterprise-level IT strategy. A company's Board of Directors should support the credit process vision articulated by the risk function, and the IT organization must in-turn support this vision. This configuration enables the credit function to meet its fiduciary responsibilities effectively and efficiently, thereby protecting the company from potential losses or unexpected liabilities.

In most organizations, the responsibility for setting enterprise-wide IT strategy typically falls outside the Credit Group's scope. However, the implementation of this strategy strongly influences how Credit Groups operate. The credit function should regularly communicate their evolving needs with the IT Group such that collaborative solutions are designed and implemented.

As a side comment; a separate CCRO white paper on "Operative Risk Resiliency for Energy Companies" is being developed at the time of this writing. It is interesting to note here that one of the early findings of that working group is that risk professionals should be increasingly working together with IT professionals, both sharing the changing needs of their function and sharing their perspectives on strategies to address them. A recurring thread throughout the entire paper, and one notably demonstrated in this chapter, is the interdependence between Credit Risk and many other functions within an organization. Credit Risk's ability to effectively work with other functions is becoming more critical as interdependence and associated information flows grow. To help facilitate enablement of the credit function through IT, best practices require appropriate governance structures and applicable IT development & maintenance operating standards. These governance structures and standard operating procedures should be informed by relevant industry frameworks. The overall IT management process requires active engagement of management from both the credit and IT functions, as well as sponsorship from senior leadership. Accountability for this process should be driven through regular status reports on applicable initiatives and on compliance with Standard Operating Procedures.

Standard Operating Procedure should be created for the credit process, updated, and regularly discussed between the IT and Credit Groups. This allows for improved transparency and coordination. The Credit Group's IT system(s) should be linked to the overall IT strategy of the organization. If it is not, the IT Group and Credit Group should revisit credit system needs and adjust the IT approach. This alignment ensures that IT Systems provide the Credit Group's needed functionality and the Credit Information Ecosystem's connectivity.

1.4.2 Robust Controls with Independence

IT and Credit Group operations should each rigorously meet their company internal business directives and applicable industry standards. Ensuring compliance with these directives and standards requires a robust Control Environment which is independent from the commercial functions.

Operating an effective and compliant credit process in today's rapidly evolving environment requires robust controls with independence. The following factors are vital to ensuring an effective credit risk control environment: (1) operate according to industry control standards and principles, (2) assure that data is transferred and processed accurately, (3) maintain periodic independent review.

The design and selection of specific controls for an IT credit system should be targeted at ensuring that data inputs and calculations are: Error-free and robust and Independent from the front office (commercial) or credit analysts

Coordination and transparency on the credit operation's control environment performance will expose any gaps or redundancies of controls across the entire Credit Information Ecosystem. With independence from the commercial function(s), the desired transparency can be achieved and appropriate actions to close gaps can be more readily taken.

1.4.3 Data Integrity

---

*To ensure the Integrity of the Credit Group's data, it should have the following characteristic: 1.*Credit and counterparty data is integrated into a single system of record*, 2.All external and internal data needed to value and manage the credit portfolio is consolidated, 3.Credit Exposure is reliably calculated and stored to support prompt reporting*

Data Integrity is one of the essential elements of a robust Credit Information Ecosystem. Without it, data immediately becomes invalidated, impacting end-user confidence at best, and at worst, could lead to material financial and reputational consequences. Ensuring data Integrity requires an "always-on" mindset, including continuous and periodic monitoring by assigned and accountable data owners.

As discussed below in greater detail, these best practices build confidence among the business functions and support critical processes dependent on this mission-critical data. They also facilitate the Credit Information Ecosystem's ongoing transformation as the industry moves toward real-time monitoring and reporting.

1.4.4 Secure & Reliable

To ensure data integrity, the entire credit IT system should be secure from unauthorized access use, disruption, modification, or destruction. Additionally, redundancy of data and critical IT systems should be put into place to ensure reliability.

While the endorsement of particular industry frameworks is generally beyond this paper's scope, the National Institute of Standards and Technologies (NIST) Cybersecurity Framework aligns with the CCRO's recommended principles.

The NIST Cybersecurity Framework, which was first established in the mid 1980s, provides IT organizations with a standardized approach for governing Cybersecurity risks. This approach offers many benefits, including a standardized control environment resulting in management efficiencies. NIST recommendations lower IT risks while delivering greater transparency and improving credit IT system reliability. Given the abundance of existing guidance on the NIST Framework, this paper addresses those specific aspects of Cybersecurity and reliability that are germane to the Credit Information Ecosystem.

1.4.5 Understood & Documented

Key elements of the Credit Information Ecosystem, including Credit Risk Models & related software applications that support credit management decision-making should be well understood by credit and IT professionals and adequately documented.

Another critical aspect of maintaining a robust credit IT system is to ensure that applicable technical and process specifications, including relevant operating Systems, databases, applications, models, dependencies be documented. While IT Groups often rely upon commercial product documentation to support their operations, this detail level is insufficient for Credit Groups that must be "audit-ready" upon demand. Company internal documentation avoids the vulnerability risk created by retention of information through just one person, ensuring that institutional knowledge is maintained.

The Ecosystem should also house and make readily available credit risk related documentation, including executed contracts, credit facility terms, parental and third-party guarantees, letters of credit, and trade credit insurance policies.

This high level of audit readiness will improve the ability to demonstrate compliance and minimize the learning curves for new IT and Credit Group personnel. For example, new IT projects addressing credit responsibilities should always include updating existing Standard Operating Procedure. This helps keep documentation up to date and employees informed of exactly how these new Systems operate.

Regularly auditing this documentation for relevancy and accuracy is also recommended. Gaps should be addressed as soon as possible, taking into consideration upcoming projects that would allow efficiency in the System documentation. Consider adding this audit step as part of the overall IT Governance processes and as a mandatory requirement of the change management process.

1.4.6 Flexible & Innovative

The entire credit IT system should be flexible to accommodate the Credit Group's evolving business needs. This includes the ability to adapt to shifts in markets, strategies, and rules. It also requires the ability to innovate using new tools and techniques.

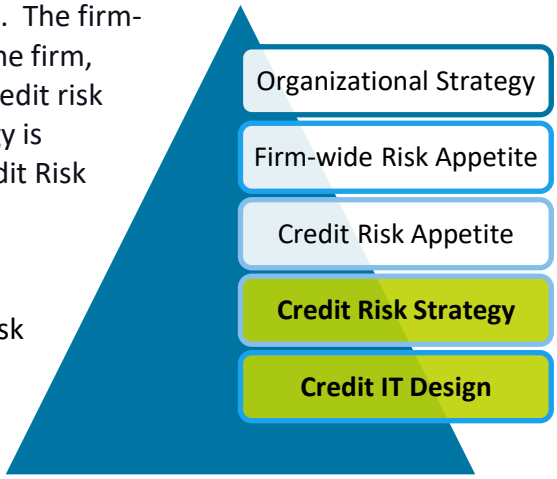
As energy business markets and technology continue to evolve at an ever-increasing rate, IT and Credit Groups must remain flexible and adaptive to these changes. Many of the changes, including automation, cloud computing, predictive analytics, and other advanced IT tools, represent a real opportunity to innovate and improve. For example, the automation of real-time (or near real-time) batch processing not only improves data accuracy by eliminating human error but also provides more timely data, reduces labor costs, and allows for personnel to focus on more value-added work.

Other credit operations benefit from innovative uses of technology include real-time or near-real-time visibility into accounts receivable balances, company Liquidity levels, and changing credit scores. See below for a further discussion on advanced technologies impacting energy credit operations.

2. Technology for Governance

2.1 Credit IT Design Aligns with Organizational Strategy

Prior to developing a Credit IT Design, a firm-wide risk strategy must be established which is integrated with the overall organizational strategy. The firm-wide risk strategy establishes a Risk Appetite for the firm, which in-turn provides an allocated appetite for credit risk specifically. To ensure a credit group's risk strategy is successful it must be aligned with the defined Credit Risk Appetite.



The credit risk function should effectively communicate its Credit Risk Strategy with credit risk professionals and other associated functions to ensure that the firm understands how the Credit Risk Strategy is effective.
In addition, the Credit Risk Committee should evaluate the Credit Risk Strategy periodically to ensure relevance and appropriateness as the organization changes over time. The evaluation should be performed Periodically to ensure that the Credit Risk Strategy still meets the firm's needs under current market and regulatory conditions.

More details on these Credit Risk Strategy concepts can be found in the previous chapter on Governance.

Most importantly for this chapter on credit IT, when the credit function has a clear, defined Credit Risk Strategy, it provides the foundation for an effective credit IT design.

> *Recommendation 1: The defined Credit Risk Strategy provides the foundation for the Credit IT Design.*

2.1.1 Board of Directors Mandate for Credit IT Design

One part of the IT organization's mission is to enable the credit function to execute its Credit Risk Strategy with success. Therefore, the Credit IT Design is so important to the credit function and to the overall firm. Only with sponsorship from executive leadership can the most effective and appropriate Credit IT Design be implemented effectively and in a timely fashion.

> *Recommendation 2: The most senior risk professional (the CRO or other head of corporate risk) leads advocacy for the Credit IT Design with the Board of Directors and senior management.*

2.1.2 Credit Risk Committee Duties/Oversight of the Credit IT Design

As discussed in the earlier chapter on Governance, the Credit Risk Committee (CRC) provides an internal management vehicle for support and oversight of the Credit Risk Strategy. The Standard Operating Procedure for the CRC should include advisory and support for the development of the Credit Risk Strategy and implementation of the associated Credit IT design. In those duties, the CRC may be informed by applicable industry frameworks and models, as discussed here in the chapter on Governance.

> *Recommendation 3: The Credit Risk Committee provides active support and advisory for implementation of the Credit IT Design.*

2.2 Designing the Credit Information Ecosystem

Now more than ever, it is critical for every organization to have an integrated data strategy to ensure the Security and Integrity of the credit-related process. Many times, these Systems will be bespoke and be in separate functions or procedures across the organization. Tying these Systems together to integrate the required data digitally is the aim of this section of the paper. This strategy may be part of a credit organization's data management plan or simply part of its overall technology design. Now more than ever, it is critical for every organization to have a data integration strategy on how to ensure data is securely shared with internal and external stakeholders. This strategic vision for Credit may be part of a credit organization's data management plan or simply part of its overall technology design.

For an energy firm to ensure this successful implementation strategy, especially when managing Liquidity Risk, it requires close coordination between the front, middle, and back-office. This coordination becomes especially important when making decisions impacting credit-related processes properly vetted across groups.

- Select the elements (e.g., people, Information System s, risk metrics, etc.) that are most appropriate for both the organization's Risk Appetite and credit portfolio;
- Implement predictive Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to act when an element is not performing as intended proactively; and

The actual credit Information Systems used by different organizations vary for several reasons, including differences in business objectives and the markets in which a company transacts. An exercise should be undertaken across the organization's different teams to discuss the credit department's primary function(s) and document what requirements and capabilities are necessary to ensure this department's success. For example, the Credit Appetite, functions, and processes will look quite different for a firm primarily engaged in Asset-Backed Trading, vs. a Regulated or Public Utility, vs. an Investment Bank, vs. an Independent System Operator (ISO).

STEP 1: Identify the Credit Group's primary roles and responsibilities;
STEP 2: Identify all stakeholders involved in the Credit Information Ecosystem, and their respective roles and responsibilities;
STEP 3: Map existing credit-related processes and Systems, including the flow of data; and

STEP 4: Identify gaps and/or technology-driven opportunities in the existing Ecosystem, and get on the IT roadmap for future investment of time and resources.

(Regarding Steps 1 and 2, the Credit Group should lead this process, and clearly document what requirements and capabilities are necessary to ensure their success.)
Once these critical roles and responsibilities are understood, then the Credit Group, with help from the IT Group and other possible resources, can focus on Steps 3 and 4, which should consider the following:

- Existing internal Systems and/or repositories that contain needed data;
- Internal Systems that can support required processes or capabilities;
- External/third party data sources that are required;
- External/third party Information System
- As necessary for needed processes or functions; and
- Evolving technology capable of improving the operations of the Credit Information Ecosystem.

(Regarding Step 4, for an energy trading business, arguably the "backbone" of a robust Credit Information Ecosystem is the Energy Trading and Risk Management (ETRM) platform, with the remainder of the "central nervous system" being comprised primarily of the Enterprise Resource Planning, General Ledger and Treasury Systems.)

The ETRM, in concert with the entire Ecosystem, should be able to perform one or more of the following primary functions across one or more traded energy products:

- Capture the primary economic terms of the deal;
- Manage and process physical logistics or movements of product, and associated documentation;
- Value transactions (e.g., Mark-to-Market, Profit and Loss);
- Document approvals and validations; and
- Compute settlement values.

Many ETRM's offer additional capabilities beyond this core set of functionalities, including, among other things, the calculation of market risk and return metrics (cross-commodity risk), calculation of Credit Exposures, hedge accounting, and compliance reporting. Additional elements of a robust Credit Information Ecosystem are discussed in greater detail below.
As the General Ledger system typically houses all financial records, integrating with the GL is crucial for getting a complete picture of the portfolio's credit status. The essential pieces of information from the GL are for credit are invoices and cash applications. Invoice data is normally straightforward to get. However, the speed and accuracy of the cash application process vary significantly across organizations. Therefore, a best practice solution would be to estimate payment of invoices based on specific rules, true up those estimates with a feed of actual cash

application, and flag any parties that are deviating from their expected behaviors outside pre-set rules.

Regardless of specific functionality, any ETRM and all Credit Information Ecosystem in general, must handle an ever-increasing abundance of both data and processing power. Given this large volume of data, both from internal operations and Systems and third-party providers, it is impossible for any organization, much less a Credit Group, to collect, organize, cleanse, manage, and interpret this data without a formalized IT Data Governance process and data management tools in place. Some typical ways to help govern credit-related data include:

- Optimize processes;
- Gain greater insight into customers, suppliers, and trading counterparties;
- Identify sources of risks and opportunities; and
- Automate decision-making using advanced technologies (Artificial Intelligence, machine learning, etc.).

The effective and efficient movement of credit-related data among the entire Credit Information Ecosystem through careful and well executed integration is thus the gold standard for success. As a result, it is not uncommon for the mapping exercise identified as Step 3 to take the lion's share of time when applying any integrated Credit Risk Management strategy, especially for the first time.

2.2.1 Automation and Analytics

The practice of automating transactions, processes and procedures using Information Systems to analyze data has been around since the dawn of computing. A compelling reason for incorporating IT into a credit processes is the benefit of decreased costs and increased efficiencies. Their most recent application in credit includes Artificial Intelligence, Robotic Process Automation, Machine Learning and Natural Language Recognition. This has resulted in the following material benefits.

- *Reduction of Labor* – Automating certain credit transactions that have traditionally been completed manually allows for those human resources to focus on other, higher-value processes that require human intervention or are not otherwise good candidates for automation.

- *Increased data accuracy* – Removing the opportunity of human error through automation improves data quality. This, in turn, improves end-user confidence and overall decision-making.

- *Decrease in Cost* – Automation of certain credit processes and procedures, such as Parametric (intraday) limit calculations, retail real-time credit evaluations, and portfolio scenarios, reduces costs in several ways. For example, the number of analysts required to assemble data to run intraday exposure position or approving retail energy customers has been substantial for companies that have automated these historically manual intensive processes.

The reduction of employees can have an exponential benefit in reducing software licensing costs, help desk time, and end-product support. Finally, automation may reduce data transaction fees and on-premise IT-related costs as cloud-based platforms become more common-place.

Credit organizations should thoroughly evaluate their IT strategies on how they can help them achieve these very real benefits of automation. As IT's goal is to enable the business, automation frequently represents an easy, quick and efficient way of realizing these labor, accuracy and costs benefits.

2.2.2 Expectations for Controls

There is no point in having controls in place if it is not possible to tell when the controls have been violated. The sooner the credit department is aware of a breach, can take faster corrective action to mitigate a non-compliant situation. Automatic monitoring of controls based on a real-time exposure calculation and immediate notification is a best practice here.
Formal procedures should be established whereby a single system owner, independent of the Front Office, sets up counter parties, commodities, products, portfolios, and locations. This ownership is often assigned to the Middle Office. This independent function should establish controls to ensure that changes to prices, volumes, and other deal terms are not permitted without proper authorization once captured within the credit system. Alternatively, if these terms are changed, the credit system should automatically alert the Middle Office that confirmation is needed. Reference data, including names, curves, models, and limits, should be reviewed periodically as appropriate (at least annually) to verify the accuracy and should be linked to or coded into the system to minimize human error. Key processes to monitor include:

- Intra-Day (Parametric) Batching: Ensure that batch processing facilitates intraday large batches of information that can be executed at low impact times for the business.

- Limits – Restrictions placed on the trading or selling Ensure that real-time processing emphasizes the ability to handle limits efficiently. Establish a comprehensive view of your firm's Liquidity, exposure, cash flows, etc.

- Violation of Limit Notifications: Ensure that the data integration design is robust and can handle notification rules.

2.3 Policy

2.3.1 Security Approach

IT Security for Credit should be addressed in several distinct manners, culminating in a cohesive approach which will provide a level of confidence that all manner of credit information is secured. Following the NIST standards is an excellent guide to achieving such a comprehensive approach. These Security approaches should be prioritized based on the overall risk associated to the credit components being addressed. Because this risk can vary project by project, the detailed summary of Security requirements are listed in the in a typical order of priority, but should be prioritized

based on the perceived risk of each Credit function. A more detailed description can be found in the IT best practices section of this paper under *"Security".*

2.3.2 Model Requirements

Information Technology models are a simple way to encapsulate standards and proven practices for conducting IT business in the Credit space without developing processes from a Greenfield Environment. While many models exist, both in the public domain and with 3rd party consulting organizations, the easiest of these models to reference as illustration of their use is the National Institute of Standards and Technology (NIST) (www.nist.org).
The NIST architectural and Security models have been around in several versions since the mid-1980s and provide IT organizations with an outlined, streamlined approach to enterprise architecture and associated Security components. Do not overlook the efficiencies and process compliance capabilities that enterprise models such as NIST could institute within IT organizations. While evaluating models, they include capabilities in the management of information, integrated Security approaches, and an emphasis on enterprise architecture standards. The more repeatable structure you can put in place with a model application, the lower the IT risk, the greater the visibility to any Security issues, and its overall benefit to operational efficiency and IT employee satisfaction.

2.3.3 System Documentation

Information Technology Systems have long been known for their lack of pertinent technical and process-related documentation. Often IT leadership rely upon commercial product documentation as a sufficient level of documentation. However, it cannot be overstated how important documenting IT Systems is as it relates to the Credit business. Operating Systems, databases, applications and their associated dependencies should be documented to a point where learning curves for new IT personnel are minimized and effective. New IT projects addressing Credit should always include activities to update existing documentation (or create new documentation as needed) to keep documentation up to date and standardized.

Documentation should be regularly audited for relevancy and accuracy. Gaps should be addressed as soon as possible, taking into consideration upcoming projects that would allow efficiency in system documentation. Consider adding this audit step as part of the overall IT Governance processes and as a mandatory requirement as part of the change control process for moving changes/updates into the production IT environment.

3. Information Technology Best Practices

3.1 Data Management

3.1.1 Single System of Record

Organizations which grow to a size where market and Credit Risk Systems are required are generally trading in multiple primary commodities, including oil, natural gas and electricity. This means that the market leading credit Information Systems are purpose-built to integrate Credit Risk data across multiple commodities. This “fit-for-purpose" functionality makes them a natural choice as a single system of record for Credit Risk data. CRMS Systems sit downstream from the ETRM’s and alongside the General Ledger or GL.

A fit-for-purpose solution that integrates all the key elements of credit operations (e.g., counter parties, trading locations, governing laws, applicable contracts and terms, and all of the exposure across all types of trading the organization, is engaged in) is vital to successfully managing Credit Exposure. This is true now more than ever as trading instruments get more complex, the global economy is further integrated, and the webs of corporate inter-relations and mergers become more intricate.
The following two Systems help maintain “the single system of record”

- *Document Management Systems* – Companies will often deploy a centralized repository that stores financial, legal, HR, and corporate documents. Most of these Systems allow external access to these documents by remote systems through a hyperlink. In instances where agreements and other credit documents are stored in such a system, the Credit Group could link to these documents for easy access.

- *Master Data Management (MDM)* - Having a single repository of all data used throughout the company would help to avoid replicating the same piece of data in multiple places. Counterparty data, including credit scores, letters of credit, and cash balances are a great example of a set of data that may end up existing in multiple places (ETRM), GL, ERPs, etc.). However, this is not often practical for larger corporations or Credit Groups operating in multiple markets. An MDM solution allows all these data sets to remain in synchronization.

Real-Time, near Real-Time, or Streaming Data

Modern advances in computing have started to allow Systems to process large datasets much faster, run processes in parallel, and incrementally update user views with new data vs. the old “wipe and reload” methods. The newer, more modern platforms take advantage of these technologies and offer credit managers the ability to perform credit analytics on a real-time or near real-time basis.

3.1.2 Batching Processes

It is the computational technique where large amounts of data are processed all at once. For Credit Systems, especially older first-generation applications, the batching processes would apply to (i) the loading of transaction records and (ii) the exposure computation process (and associated analytics). Since these processes can take a significant amount of time (up to multiple hours for large data sets), companies will typically schedule this once-per-day. Usually, at night, few or no individuals would be accessing the system. This results in firms managing risk on a T+1 basis. While sufficient for many organizations, this time lag does have some significant drawbacks for others. Some firms attempt to bypass this limitation by running multiple (sometimes smaller) batches during scheduled times throughout the day. This can be problematic for trading desks that are very active or operate in multiple geographic markets and need a more real-time view of their credit positions and exposures to make trading decisions and cannot afford their system to be out of commission hours each day.

For this reason, newer generation platforms offer real-time (or near real-time) processing that allows the user-facing portions of the system to run continuously. In contrast, the extensive computational processes run in the background and update what the user sees as they are completed.

3.2 Elements of an Integrated Credit Information Ecosystem

3.2.1 Exposure Calculation Attributes

The calculation of Credit Exposure is the primary purpose for any credit system. The particulars of these exposure calculations are covered in various other sections of this paper (e.g., netting terms by contract are covered in the contract section); however, a few general best practices are addressed below when considering calculating exposures in some type of credit system.

- *Accuracy and Operability* - Credit groups should always be able to promptly answer the question, "How much money will be lost if (Company X) goes bankrupt?" The primary purpose of a credit department is to mitigate credit-default losses. This entails the ability to calculate the size of a potential loss quickly and accurately. As well as the agility to look at exposures contractually and operationally. A Credit Risk Management System can help enable these capabilities.

  For example, it's frighteningly easy to lose sight of operational exposure in the wake of bull markets whose duration can be measured in decades. Conversely, carefully tracking and managing Credit Risk becomes even more critical during extended positive market runs to the point of being a competitive advantage as recent events have exposed in a handful of cases.

  Many companies use an exposure calculation, which does not reflect their contractual obligations in the event of a default. They may instead look at the exposure

operationally. Usually, this approach involves assuming both deliveries before but not yet invoiced, Balance of the Month Exposure (BalMo), and invoice's payment.

There is nothing wrong with using this type of "operational" view of exposure. For example, calculating the rolling 60-day Credit Exposure window is common practice in the oil and gas industry. These calculations are a reasonable proxy most of the time. Still, they usually differ from what a company would be owed or owe in the event of an actual counterparty default. Depending to what extent the company is obligated to continue to deliver through a default. Therefore, the practice of calculating multiple "looks" at exposure is recommended, given the capabilities and low cost of today's computing power.

- *Functionality* - Thoughtfully choose the tools that your company implements as part of its credit policy and understand those tools' strengths and weaknesses.

  The alphabet soup of analytics that can be used, combined with the decreasing cost of computing power, can make it seem attractive to implement everything. However, more is not always better. The more metrics that a credit analyst is exposed to, the less attention they will pay to the critical ones. Therefore, evaluate the needs of your company based on the risks present in the portfolio. Then determine the best measures for your organization to take and predictively mitigate those risks.

  For example, the accurate calculation of a credit reserve amount is more important (in terms of remaining solvent) for a smaller company in a middleman trading position than for a larger company originating some commodity with $1 billion of cash on hand. This does not mean it is bad for the large company to calculate its credit reserve. But they should probably be more focused on Potential Future Exposure (PFE) limits and PFE change day-over-day in total and Book Value.

  Conversely, this does not mean the small company should not be calculating PFE, but knowing about potential future issues is not relevant if you cannot survive a default today.

- *Reassessment* - Impose a regularly scheduled review to ALL exceptions to the credit policy at some interval that makes sense.

  This applies especially to exceptions that have been implemented in a system as they may escape notice. Ideally, each exception's review period should also be coded into the system in the same way that the exception itself is coded. For example, if a trade is ignored when importing exposure, add some automated notification/workflow/message to review the logic behind neglecting it. This practice helps preserve institutional knowledge and mitigates the risk associated with shift changes, staff turnover, and the business's general press.

- *Audit-ability:* Do not allow non-audited Credit Exposure adjustments of any kind.

3.2.2 Integrated Margining System

With companies growing more sensitive to how available cash is being leveraged, there has been an increase level of scrutiny on margining. There are three best practices to calculating margin correctly, including:

- *Connection to ETRM System(s)* - The first practice is having a promptly available and accurate valuation of the Credit Exposure that's subject to margining. This practice requires having a direct and automated integration with system(s) providing portfolio valuations.

- *Integrate with Treasury Systems (GL) & Bank Facilities* - The second practice is knowing your collateral position by each marginable contract by using as much data as possible directly from the system of record. Separating the margin cash from invoice payments by legal entity and contract is more of a hypothetical perfect state rather than a common practice. A more reasonable best practice is to verify the total cash received compared to the sum of expected receivables and total margin for the given entity or legal family.

- *Automating Margining Calculation* - The third practice is to automate the calculation of margin to ensure accuracy and reliability. Ideally, your automated margining platform should support:

  - Capture of common credit margining terms in your major areas of operation;
  - Support for exposure calculation modification to account for common modifications in your area of operation;
  - Automatic generation/distribution of margin calls;
  - Provide an operational summary of expected activity for the day – what the analyst needs to do and expect from parties;
  - Provide a report of all marginable contracts and associated metadata (e.g., exposure against contract, collateral in transit, current outgoing and expected incoming margin calls, etc.);
  - Ability to exclude / include transactions from margining; and
  - Support for dispute resolution.

3.2.3 Integrated Contracts

Contracts are another key element of an integrated Credit Information Ecosystem. The following are two key practices to consider in this area:

- *Contract Credit Terms* - All key credit-related contract terms, including relationships between contracts (set-off language) and relevant governing law, must be captured, and incorporated into the calculation of Credit Exposure to ensure accuracy.

- *Linked with Margining System* - The terms Margining collateral must be incorporated into the Credit Risk calculation, and an automated link with the margining system to import collateral position is the standard here.

3.2.4 Integrated Credit Scoring Process

The general concept of reviewing the creditworthiness of a trading partner has been important since trade was invented. The best practice is doing everything possible to understand your trading partners before engaging in business and then regularly evaluating the partner's health and the relationship.

The tools to accomplish this can

- *Financial Statement Data* – Raw information obtained from public sources or the trading partner.
- *Ratios and Weightings* – Calculations based on the raw information
- *Qualitative Assessments* – Subjective measures such as the length of the relationship.

The use of third-party management software tools can help automate the credit scoring process, both during on-boarding as well as part of on-going monitoring. For example, these tools can automate the counterparty review process and ensure relevant reports occur on a timely basis. This relieves analysts of the repetitive work of third party-related data collection and calculation while providing they are done thoroughly, accurately and, timely. This leaves more time for the analyst to work the more subjective aspects of the credit review process, which cannot be automated, and leads to a better overall result.

3.2.5 Digitalization of Credit Documents

As a best practice, credit analysts should have easy access to electronic copies of documents relevant to credit. This would include such things as contracts executed with trading partners, credit facility terms, parental and 3rd party guarantees, Letters of Credit, and Trade Credit Insurance policies amongst others.

This applies regardless of whether a credit system is being used as no system will have out-of-the-box capacity to capture the full nuance of all the listed items in all cases.

3.2.6 On-Boarding System and Processes

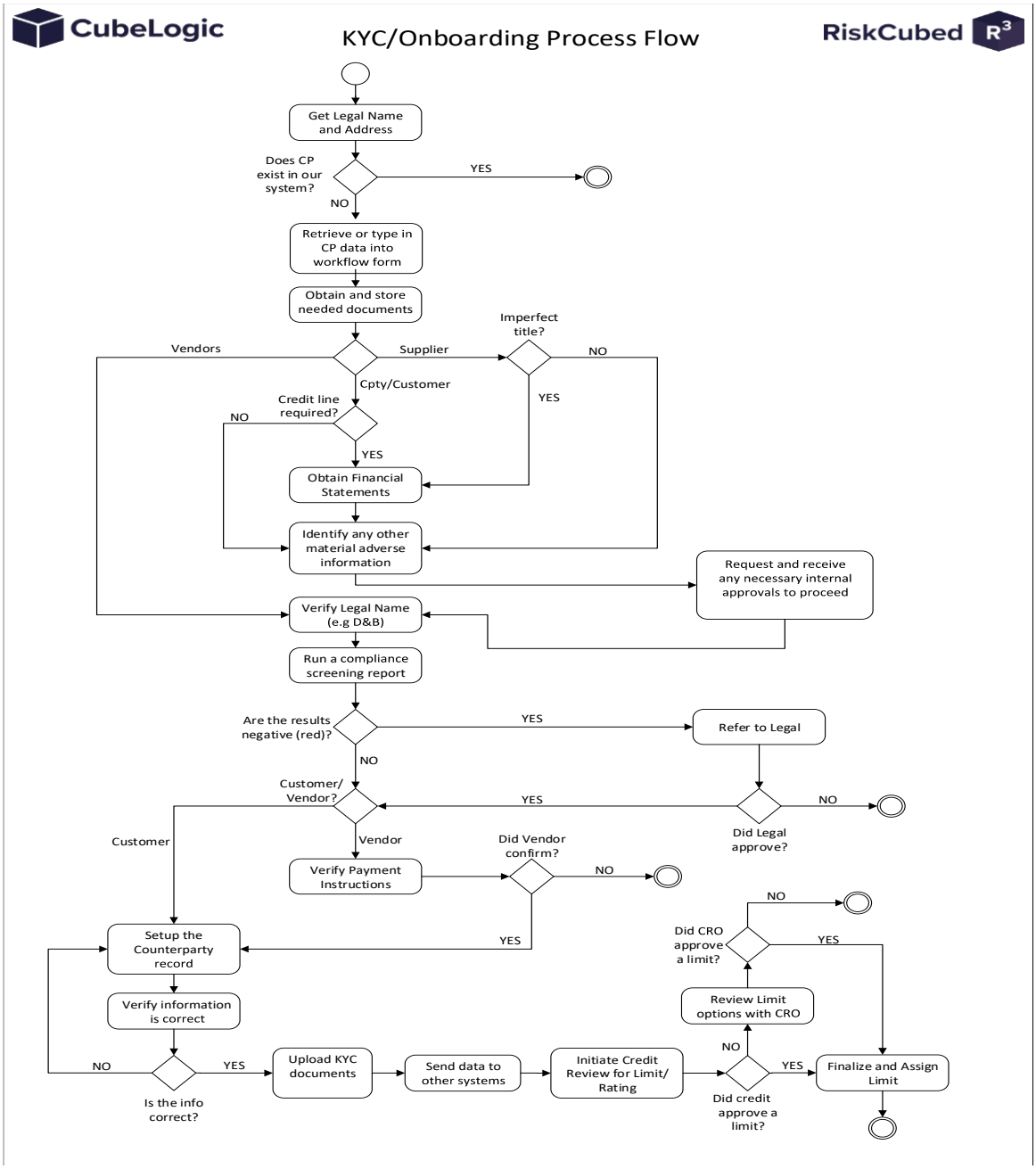
Data On-Boarding can generally refer to any exercise where a new data object is set up or initialized. For credit functions, this typically means the On-Boarding of new counterparties or customers.

KYC or "Know Your Customer" laws were introduced in 2001, but the general concept of understanding who you are in business with has been important since trade was invented. The best practice is doing everything possible to understand your trading partners before engaging in business and then regularly evaluating the partner's health and the relationship.

- *Requirements* - Each organization has its unique way of doing business, its own internal processes and Systems, and its own organizational structure. This means that chief among all requirements is an ability for the onboarding tool to be flexible and configurable. Onboarding by nature is a multi-step workflow process requiring input from multiple departments and individuals. Along the way, this process will require the collection of disparate data elements (e.g., reference data, checklists, individual documents, approval stamps, etc.), commentary from the individuals involved, (potential) interaction with external data services, and more.

- *Information Workflow:* The tool should allow the user to design their process flow, have a clear structure to move from one step to the next (or skip steps), allow for configurable rules to be designed and managed, have a facility to custom-design the layout of the screens for each step in the workflow, integrate with email for remote interaction, APIs to external data services, seamlessly interact with the rest of the system to populate drop-down lists, and more. See Figure 2 below for an illustration of a hypnotical On-Boarding workflow.

Figure 2: KYC/On-Boarding Workflow



3.3 Cloud Services

Today most mid-to-large sized companies can realistically target 70-80% of their overall Platform to be cloud-based. The remainder of the on-premise need for an infrastructure platform typically stems from legacy, commercial-off-the-shelf (COTS) products that are of older architecture and have

become business-process critical or are otherwise not on an organization's go-forward Standard Operating Procedure. As time progresses and priorities dictate, these solutions are expected to be updated, resulting in these same mid-to-large sized companies closing the gap towards a complete cloud-based Platform in the near future.

During the design phase of any cloud platform project, significant consideration should be how Cloud Providers may be leveraged beyond the given project's immediate need and scope. Deciding on a Cloud Provider only based on a current set of high-priority requirements may ultimately lead to longer-term challenges, including higher total costs and difficulties supporting these platforms. A good portion of each Cloud Provider's functionality is based on other technologies, such as multiple application and website hosting services. These capabilities need to be considered today for future IT Standard Operating Procedure activities.
The cloud platform environment is constantly changing and evolving. Given this current change pace, it is recommended to limit cloud platform decisions to a 3-year perspective. These platforms have a significant ability to impact IT's capability to provide robust, efficient functionality to Credit's business and need to be carefully managed.
In a recent publication of CIO Magazine, a relevant quote is worth considering:
"A best practice is to ensure that for all requested Cloud Service, [the services] are subjected to proper architecture and Security reviews on any IaaS, PaaS, or SaaS vendor platforms, before being approved for use in the enterprise." Smith says. "Guidance and guardrails must be established before any public cloud vendor tools can be provided to the organization, including ongoing monitoring of all usage."
"IT, Cybersecurity, and legal must all work together to keep in front of all efforts of business users to procure and consume new Cloud Services," Smith says.

3.4 System Security and Redundancy

3.4.1 Data Security

- *Physical Security* - As obvious as it may appear, physically securing an IT system often tends to be a frequently overlooked requirement for ensuring overall IT security. As IT Systems become further distributed physically–on-premise, cloud-based, a hybrid of both, or even 3rd party hosted elements – it becomes crucial to adopt a thorough Physical Security approach. Physical Security should consider, at a minimum mechanism for access/egress to physical computing components such as servers, storage arrays, networks/routing devices, or platforms may have unrestricted or quickly accessible access to these components. A large portion of Security breaches occurs simply because someone can walk onto a premise and physically plug a cable into the network.

  Regular audits of who has physical access to credit IT physical resources this proactive step minimizes the exposure and risk associated with IT security.

Implementation of a two-person approach to managing any data being physically removed from any system allows a checks-and-balances approach to ensuring data security. Transportation outside of any data center and or secured facility should consider guards to secure sensitive data safety.

- *Logical Security* - IT Systems, in general, do not always require physical access but always require logical access of some sort. Whether this is due to some defined Access Control List (ACL) or simply being able to extract and store data outside of its typical means, all of these represent Logical Security challenges. Consider putting the following processes into place to address Logical Security.

  Make reviewing ACLs a regular part of the IT Governance process.
  Consider expiring access as default instead of granting access indefinitely. While this may create a small amount of additional overhead from an IT perspective, reducing the risk associated with unsecured logical access is typically considered well worth the tradeoff.

  Secure credit data and related information in the smallest but most business-aligned Logical Security buckets. By putting this more advanced level of Security into place, it minimizes the total amount of data that could be exposed during any IT Security breach.

- *Security Governance* - Not typically considered part of the Security portfolio, IT Governance is not to be overlooked as the overall encompassing guidance for IT Security. Research into many historical Security breaches has determined that if an overall IT Governance process had been in place, the Security breach would likely not have occurred or would have occurred at a lesser severity. Several key elements of the Security Governance process that should be considered are:

  – *Information Lifecycle Management* – Easily accessible data should be limited by archiving or otherwise making data less accessible. This limits data exposure during any Security breach while still allowing data to become accessible if needed.

  – *IT Architecture Reviews* – Formation of an IT Architecture review board exposes individual Information System architectures to a more systematic and holistic review process. For example, internal threats to Security to Systems can be mitigated in this fashion. Any inconsistently applied Security mechanics can be found and corrected before these Systems being placed into production.

- *Security Patching* - Every IT system hosting credit-related information should be placed on a platform requiring regularly patched operating Systems and application environments to remain fully functional and secure. This ensures that a patching process is in place that addresses patching needs in a time-effective manner while balancing credit business uptime with the risk and Security of IT system patching.

3.4.2 Controls

A vital component of a Credit Information Ecosystem is the ability to create a robust control environment. This system should be used to capture credit ratings, manage limits, document approvals, provide credit documentation, and calculate exposure and return metrics. The actual system may vary by the company because of differences in business objectives and the markets in which a company makes transactions.

Best practices for controls include:

- Employee access to the system should be limited, and Security should be established by location, application, function, and data;
- Security clearances should be approved by direct supervision;
- Formal procedures should be established whereby a single system owner, independent of the front office, sets up counterparties, commodities, products, books, and locations;
- Reference data (contract information, exposure, models, limits, etc.) should be reviewed periodically as appropriate (at least annually) to verify accuracy and should be linked to or coded into the system to minimize human error;
- The Credit Informational Ecosystem should be able to capture all transactions or provide credit rating, disaggregate risks by contractual obligation, credit terms, capture GL information, calculate PFE, concentration risk in the portfolio, calculate credit charge, set user Security by portfolio segmentation, and contain a detailed audit trail/changelog by user ID;
- Controls should be established to ensure that changes to counterparty data, confirmations, and other deal terms are not changed without proper authorization once captured. Alternatively, if these terms are changed, the system should alert the middle office that confirmation is needed;
- All mission-critical systems should have 24-hour availability and should be backed up systematically once a day at a minimum;
- All data storage be kept in a secure location.; and
- Complete business continuity plans should be maintained and tested and should include a site to continue operations if events prevent access to the trading floor.

3.4.3 System Documentation

Modern Systems are not static, and they evolve over time. A review should occur regularly to ensure that all the critical system documentation is up to date. This eases the onboarding of new credit analysts and ensures operational continuity in a disaster or the normal churn of staff over time.

3.4.4 Auditable Change Record

Monitoring all changes in the system (configuration, business data, etc.) is necessary for most audits and assists in troubleshooting business and technical problems. Particular to credit, being

able to generate historical views is helpful so that decisions can be explained in terms of what data was available when the decision was made.

3.4.5 Version control

Version control is a process designed to keep track of multiple versions of software. Any system that provides change tracking and control over software and documentation can be considered a version control process. The practice has been a part of software development or printed material almost as long as writing has existed.

The purpose of version control is to ensure that the software's content changes are documented, and the effects open to other components within the Credit Information Ecosystem are understood. At the same time, version control is often carried out by a separate application, word processors, and spreadsheets. Version control allows servers in multiple locations to run different versions on different sites, even while those versions are being updated simultaneously.

3.5 Advanced Information Technology

Customarily, IT strategies have revolved around the "enablement" of business roles such as Credit Risk managers, analysts, and risk professionals to perform their day-to-day tasks. Today, advanced IT strategies focus on growing data maturity, which ultimately leads to a higher level of confidence in reports and analytics sourced from the core datasets. The following Advanced IT concepts provide unique insights and opportunities affecting Credit Risk management.

3.5.1 Artificial Intelligence (AI)

Often, AI is associated with sci-fi movies and is more recently drawing calls for increased regulation to limit perceived threats. However, when applied appropriately, AI can facilitate more benign Credit Risk functions, including evaluation, planning, calculations, analytics, and decision-making.

3.5.2 Machine Learning (ML)

This is a subset of Artificial Intelligence and contains a baseline or starting point in mathematics and statistical algorithms. Machine learning depends on learning over time and typically performs best when provided with large, diverse amounts of data from which to "learn". ML involves the following three areas:

- Predictive Analysis – As the term "predictive" describes, these models are used to provide insight into future events, patterns, and trends. A typical business implementation of Predictive Analytics
- involves decision trees where the system "learns" from past decisions and outcomes and uses it to "predict" the future path for success.

- Data Mining – Think of Data Mining similarly to commodities mining, such as coal ore, oil, etc. This is the processing of large amounts of randomly stored data to extract valuable components. Typically, the output from Data Mining is input into other advanced data techniques. Therefore, the better the Data Mining tasks are performed, the better subsequent business decisions can be made. Data Mining sources include emails, transactional Systems (for trends, etc.), social sentiment (such as Twitter, Facebook, Glassdoor, etc.). When done appropriately, Data Mining will also associate other 3rd party data to the data being mined. Examples of this include: Pulling in weather patterns when certain business-level events occur, storing traffic patterns and transportation issues when deliveries are delayed, etc.

- Deep Learning – An approach where decisions are formulated based on a series of layers. Each layer performs a specific task and no more. This allows that layer to learn from a minor decision point and thus becomes much more proficient at its task than from a more significant, more complex task. The concept of "deep" implies that hundreds or thousands of layers can be automatically generated as your Systems continue to learn. Over time, they can successfully predict the appropriate paths instead of having to transverse each layer.

3.5.3 Shared Ledger (Block Chain)

Within the last four to six years, Blockchain technology has been at the forefront of a technology set attempting to solve a reasonably universal issue: secure information or transactions in a manner that cannot be modified outside of secure, authorized channels. Blockchain's largest market currently is in the FinTech space, it also has an important place in the commodity and energy markets and throughout the energy supply chain.

- *Example* - Recently, a gas and fuel distribution chain has teamed up to create a broad Blockchain implementation strategy to help prevent fraud and theft. As fuel theft has a worldwide impact of over $1b per year, having a way to securely trace and verify these types of transactions has become very important. This works because Blockchain Shared Ledger entries are used from the refinery to the delivery vehicle and from the delivery vehicle to the station tank. At each handoff, a new "block" was added to the Blockchain with amounts transferred and the product's quality. This allowed both the supplier and customer to understand if/when theft or a lower-quality product was introduced. This initiative was seen as a quality improvement service to the supplier's offering that differentiated them from other suppliers and provided confidence to the customer that they are receiving the quantity and quality of the product they purchased. One can expand this application into the Natural Gas pipeline world, as an example, where dealing with tariffs, injection sites, and varying pressurized pipelines introduces different levels of quality.

3.5.4 Natural Language Processing (NLP)

A sub-field of AI, NLP facilitates a "natural" way of communicating between humans and computers/machines. While there are many options for the deployment of an NLP system, the most common implementation is in the form of "Chatbots. These virtual assistants mimic a human personality and attempt to answer common questions that end users may ask. From a business perspective, this alleviates people's need to engage either online or via phone directly. Additionally, it minimizes exception processing, improves the quality of data captured, and consistently applies business rules to any conversation. Much like other advanced IT processing of data, the quality of interaction is directly driven by the amount and quality of data that these virtual assistants have access to "learn."

3.5.5 Digitization of Credit Process

The Lack of The Credit Process's digitization is tremendously risky in itself. While many actions and activities have moved into the digital world, for technologies such as AI, ML, and others to provide the most valuable, all aspects of the Credit Process must be digitized. Often, exceptions and other one-off processes are handled manually, and thus their digitization – and the logic that formulated those decisions – are not "learned" by the Advanced IT techniques.

3.5.6 Conclusion

Advanced IT techniques can help credit professionals draw insights from vast volumes of market data and support credit decisions more than traditional analog approaches. Energy companies can no longer exclusively rely on humans to establish direct parameters & rules for algorithms or other data-intensive activities. Allowing Advanced IT techniques to derive more profound insights into your data while the credit analyst remains responsible for credit valuation and mitigation.

4. Glossary of Terms

Access Control List) - A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.
Artificial Intelligence (AI) - The development of applications, subroutines or other automated means that mimic the decisioning and logic leveraged by humans.
Asset-Backed Trade - The asset-backed trading is a style of commodity trading which is used to seek and exploit market volatility in order to monetize the operational assets owned by the trading entity.
Balance of the Month Exposure (BalMo) – The remaining days left in the month in which a commodity has not yet been delivered to the customer/counterparty. The Credit Exposure for the remaining undelivered days in the month is calculated using a MtM valuation method. A creditor will not continue to delivery to a counterparty if a default event has transpired unless they are contractual obligated to so. MtM calculates the replacement costs to the creditor if the undelivered commodity value is "Out of the Money" to the current market price.
Bank Facilities - A facility is a formal financial assistance program offered by a lending institution to help a company that requires operating capital. Types of facilities include overdraft services, deferred payment plans, lines of credit (LOC), revolving credit, term loans, letters of credit, and swingline loans. A facility is essentially another name for a loan taken out by a company.
Billed – Invoiced receivables for product that has not yet been paid by the counterparty or Customer. A component of the Current Exposure calculation.
Blockchain (see Shared Ledger) - An architecture of a series of "blocks" that leverage cryptography to ensure a secure, two-party transaction in an approach that is verifiable and permanent. There are various implementations and architectures of Blockchain, depending upon the industry and specific use.
Book Value - The Book Value of a company is the net difference between that company's total assets and total liabilities, where Book Value reflects the total value of a company's assets that shareholders of that company would receive if the company were to be liquidated.
Chatbot- A phrased coined for a "virtual assistant" typically rendered by webpages or applications. These chatbots attempt to answer human-authored questions that represent typical questions from their users. The intent of a chatbot is to reduce or eliminate load on humans supporting the application and/or industry, forming a more cost-effective approach for the company and a more consistent experience for the customer.
Cloud Providers - A cloud provider is a company that delivers cloud computing-based services and solutions to businesses and/or individuals. This service organization may provide rented and provider-managed virtual hardware, software, infrastructure, and other related services. Cloud services are becoming increasingly desirable for companies because they offer advantages in terms of cost, scalability, and accessibility.
Cloud Services - Cloud services refer to any IT services that are provisioned and accessed from a cloud computing provider. This is a broad term that incorporates all delivery and service models of cloud computing and related solutions. Cloud services are delivered over the internet and

accessible globally from the internet. There are three basic types of cloud services: Software as a service (SaaS), Infrastructure as a service (IaaS), Platform as a service (PaaS).

Cognitive Analytics - Intelligence and analytics based on Artificial Intelligence and Machine Learning. This set of information focuses on scenarios where there may be other influencers or variables that are not currently known.

Computer Security Resource Center (CSRC) - Provides the public with NIST resources on computer, cyber, and Information Security and privacy.

Confidence Interval - A measure of the degree of confidence, or equivalently the probability that is associated with the set of outcomes, for a random variable (or a stochastic process) of interest. A confidence level of α is defined as the probability that, given the underlying distribution of the random variable (or process), the set of possible outcomes will lie in a range greater than or equal to a predetermined value. Equivalently, a confidence level of (1 – α) is defined as the probability that the set of outcomes will lie in a range less than or equal to a predetermined value. As an example, a confidence level of 5% is used to assess the set of possible outcomes and assign a probability of 1 in 20 that the actual outcome will lie above a predetermined value, the latter being a function of the underlying distribution and the level of confidence being used. Alternatively, a confidence level of 95% is used to assess the set of possible outcomes and assign a probability of 19 out of 20 that the actual outcome will lie below the predetermined value.

Credit Exposure – Is the sum of Current Exposure and Potential Future Exposure.

Credit Group – the credit department of an organization, including any key stakeholders to the credit function (for example the Chief Risk Officer and/or the Chief Financial Officer). Depending on the size and sophistication of the credit function, this could include credit analysts, credit managers, directors of credit, and Chief Credit Officers.

Credit Information Ecosystem – Is all encompassing term that captures all aspects of the counterparty/customer, data, processes, and System s tasked with managing credit risk. It would include items both external and internal to the organization and it is understood that individual components within the Ecosystem, as well as the System would likely evolve over time. The components in the Ecosystem include, but are not limited to, the credit team, senior management, all credit-related data, 3rd party entities (banks, data providers, insurance providers, exchanges, etc), System s and other software tools, and business processes."

Credit Risk - Credit risk is the market risk exposure to its counterparties or customers' credit quality. The risk is the counterparties or Customers' ability to make contractual payments or deliver a specified energy commodity, product, or service. For instance, a trading operation may purchase a forward position from counterparty A to hedge an open position, but if counterparty A defaults, the previously hedged position may run afoul.

Credit Risk Management System - (CRMS) - The integrated System responsible for managing data specific to the credit department and for producing the Credit Exposure. Typical data and processes managed with the CRMS include counterparty (or 3rd party legal entity) data, contract terms related to credit (e.g., netting terms, covered products, adequate assurances, material adverse change clauses and others), collateral (e.g., letters of credit, guarantees, credit support annexes, etc), credit limits, credit analytics, and credit reporting.

Cross-Commodity Risk - Cross commodity hedging or cross hedging represents a risk trading strategy when a trader trades hedge positions on two positively correlated commodities

(securities) with similar price movements. When a positive correlation shows that two commodities move in the same direction, such as gold and silver, Crude Oil, and natural gas, etc., a trader can buy one commodity and sell another commodity to reduce risk.

Current Exposure – Is the initial financial loss a creditor could lose in the current period from the default of a counterparty or customer. Current exposure is comprised of (Delivered but Unbilled + Billed + MtM)

Cybersecurity – Is the combination of people, policies, processes and technologies employed by an enterprise to protect its cyber assets. Cybersecurity is optimized to levels that business leaders define, balancing the resources required with usability/manageability and the amount of risk offset. Subsets of Cybersecurity include IT security, IoT security, Information Security and OT security.

Data Governance - A set of processes that ensures that data assets are formally managed throughout the enterprise. A Data Governance model establishes authority and management and decision-making parameters related to the data produced or managed by the enterprise.

Data Infrastructure - A Data Infrastructure can be thought of as a digital infrastructure that is known for promoting data consumption and sharing. A strong Data Infrastructure enhances the efficiency and productivity of the environment in which it is employed, increasing the collaboration and interoperability.

Data Mining - The extraction of data from large amounts of data in a set and repeatable pattern. Typically used for identifying trends and patterns more than analytics of what the outcome may provide.

Deep Learning - Leveraging Machine Learning, Deep Learning tiers multiple layers of machine thought and decisioning upon one another, forming a sort of neural network of logic. Each layer is allowed to operate independently upon one another, allowing a large range of variables that are considered at each step.

Descriptive Analytics - Intelligence and analytics that answers "what has happened." This typically only references outcomes from a historical perspective.

Diagnostic Analytics - Intelligence and analytics that answers "why did it happen." This typically only references outcomes from a historical perspective.

Energy Trading and Risk Management (ETRM) - System s involves commercial decision making and market execution using an integrated System that enables data exchanges among trade floor, operations, credit, contract, and accounting functions. Integral to the process are event and trade identification/capture, comprehensive Risk Management strategies/policies, scheduling/nomination/transportation, and settlement execution. The process also provides for price transparency, market monitoring, controlled access, and regulatory compliance.

Expected Exposure - Average market value on future target date. Equivalent to 50% Confidence Interval.

General Ledger (GL) - Is the record-keeping System for a company's financial data with debit and credit account records validated by a trial balance. The General Ledger provides a record of each financial transaction that takes place during the life of an operating company.

Greenfield Environment – Developing a System for a totally new environment, without concern for integrating with other System s, especially not legacy System s.

Independent Service Operator (ISO) - An independent, federally regulated entity established to coordinate regional transmission in a non-discriminatory manner and ensure the safety and reliability of the electric System.

Information Lifecycle Management (ILM) -Is an approach to data and storage management that recognizes that the value of information changes over time and that it must be managed accordingly. ILM seeks to classify data according to its business value and establish policies to migrate and store data on the appropriate storage tier and, ultimately, remove it altogether. ILM has evolved to include upfront initiatives like master data management and compliance. (Gartner IT Glossary)

Information Security - The protection of information and Systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, Integrity, and availability.

Information Security Architecture - An embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, security Systems, personnel, and organizational subunits, showing their alignment with the enterprise's mission and strategic plans. See Security Architecture.

Information Security Risk - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or Systems.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology (IT) - Any services, equipment, or interconnected System (s) or subsystem (s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information Technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information Technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Investment Bank - Investment banking is a specific division of banking related to the creation of capital for other companies, governments, and other entities.

IT Architecture - A framework and set of guidelines to build new System s. IT architecture is a series of principles, guidelines or rules used by an enterprise to direct the process of acquiring, building, modifying, and interfacing IT resources throughout the enterprise. These resources can

include equipment, software, communications, development methodologies, modeling tools and organizational structures.

IT Governance - Is the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals.

IT Infrastructure - IT infrastructure is the System of hardware, software, facilities, and service components that support the delivery of business System s and IT-enabled processes.

IT System - A collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT System resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. An IT System may consist of one or more computers and their related resources of any size. The resources that comprise a System do not have to be physically connected.

Key Performance Indicator (KPI) - Are a set of quantifiable measurements used to gauge a company's overall long-term performance. KPIs specifically help determine a company's strategic, financial, and operational achievements, especially compared to those of other businesses within the same sector.

Key Risk Indicators (KRI) - Key Risk Indicators are used by financial firms to measure their exposure to a given risk at a particular time. By comparing an appropriate set of Key Risk Indicators with internal limits and thresholds, banks can determine whether their operational risk exposures are within their Risk Appetite.

Liquidity Risk (Collateral) - In the context of funding, Liquidity Risk refers to the ability of organizations to fund liabilities as they fall due without incurring losses through being forced to sell less-liquid assets quickly.

Liquidity Risk (Market) – In the context of traded markets, Liquidity Risk is the risk of being unable to buy or sell assets in each size over a given period without adversely affecting the price of the asset. The risk will be high if, for example, a large trade is being executed over a short period of time in an insufficiently liquid market.

Logical Security – Safeguards for an organization's IT System s, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users can perform actions or access information in a network or a workstation. It is a subset of computer security.

Machine Learning (ML) - Like Artificial Intelligence (AI), but focuses on historically and automatically improving logic and decisions over time based on prior execution of the algorithm(s).

Mark-to Market (MtM) - The value of a financial instrument (or a portfolio of such instruments) at current market rates or prices of the underlying product. Constitutes the current replacement costs of future deliveries or financial settlements. A component of the Current Exposure calculation.

Master Agreements - Is a contract that spells out most but not all the terms and conditions between the signing parties. Its purpose is to speed up and simplify future transactions. The initial time-consuming negotiation is done once, at the beginning. All future transactions are done with a confirmation and fall under the Master Agreement. Confirmations spell specific transaction,

price, quantity excreta. All transactions are governed under one master contract. Examples of common commodity Master Agreements are EEI, ISDA and NAESB.
Maximum Exposure – Is the highest potential credit loss from the default of a counterparty or customer. Equates to a very high Confidence Interval such as 99%.
National Institute of Standards and Technology (NIST) - A unit of the U.S. Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

Natural Language Processing (NLP) - An artificial intelligence-based approach for helping computer System s understand interaction mechanics with humans. This typically involves language and pattern recognition, and is typically implied through the means of "chat bots," though there are numerous other applications for NLP.

Parametric - The Parametric method, also known as the variance-covariance method, is a Risk Management technique for calculating the VaR of a portfolio of assets that first identifies the mean, or expected value, and standard deviation of an investment portfolio. The Parametric method looks at the price movements of investments over a look-back period and uses probability theory to compute a portfolio's maximum loss. The variance-covariance method for the value at risk calculates the standard deviation of price movements of an investment or security. Assuming commodity prices and volatility follow a normal distribution, the maximum loss within the specified confidence level is calculated.

Physical Security - Physical security describes measures designed to ensure the physical protection of IT assets like facilities, equipment, personnel, resources and other properties from damage and unauthorized physical access. Physical security measures are taken to protect these assets from physical threats including theft, vandalism, fire and natural disasters.
Potential Future Exposure (PFE) - PFE is the stochastic model method estimating potential credit loss on a future date with a specified confidence interval.
Predictive Analytics - Intelligence and analytics that attempt to predict specific outcomes based on historical data.
Profit and Loss (PnL) - Is the day-over-day change in the value of a portfolio of trades typically calculated using the following formula: PnL = Value today - Value from Prior Day
Regulated/Public Utility - A regulated or public utility company (usually just utility) is an organization that maintains the infrastructure for a public service (often also providing a service using that infrastructure). Public utilities are subject to forms of public control and a regulation ranging from local community-based groups to statewide government monopolies.
Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of Occurrence.
Risk Assessment - The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a System.

Risk Management - The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Risk Tolerance/Appetite — An organization's willingness to absorb declines in the value of an asset while pursuing its objectives and before any action is determined to be necessary in order to reduce the risk

Security - A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of System s. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's Risk Management approach.

Security Architecture - An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, Information Security Systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

Security Control - The safeguards or countermeasures prescribed for an Information System or an organization to protect the confidentiality, Integrity, and availability of the System and its information.

Security Requirement - A requirement levied on an Information System or an organization that is derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, Integrity, and availability of information that is being processed, stored, or transmitted.1

Security Governance - Security governance is a process for overseeing the Cybersecurity teams who are responsible for mitigating IT business risks. Security governance leaders make the decisions that allow risks to be prioritized so that security efforts are focused on business priorities rather than their own. They also govern the interplay of mitigating identified IT business risks, addressing internal and external threats, and dealing with compliance.

Security Patching – Is an update that is pushed from a software developer to all the devices that have the software that needs the update. The reason for these delayed patch updates is because the hole or vulnerability is not discovered before the major update or initial software is released. The purpose of a security patch update is to cover the security holes that a major software update or initial software download did not.

Shared Ledger - (see Blockchain)

Standard Operating Procedure (SOP) - A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event.

1 *(Note: Security requirements can be used in a variety of contexts from high-level policy activities to low-level implementation activities in System development and engineering disciplines.)*

System - Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.234 See Information System.
Trustworthiness - The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.
Trustworthy Information System - An Information System that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.
Unbilled - Receivables for product that has been delivered but not yet invoiced. A component of the Current Exposure calculation.

2 *(Note 1: Systems also include specialized System s such as industrial/process controls System s, telephone switching and private branch exchange (PBX) System s, and environmental control System s. Combination of interacting elements organized to achieve one or more stated purposes.)*

3 *(Note 2: There are many types of System s. Examples include: general and special-purpose information System s; command, control, and communication System s; crypto modules; central processing unit and graphics processor boards; industrial/process control System s; flight control Systems; weapons, targeting, and fire control System s; medical devices and treatment System s; financial, banking, and merchandising transaction Systems; and social networking Systems.)*

4 *(Note 3: The interacting elements in the definition of System include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities.)*

5. Index

6. References

CCRO (2002), "*Volume 6 of 6 Glossary*", Publication of Energy Risk Best Practices by the Committee of Chief Risk Officers

Gartner, (2021), "*Information Technology Gartner Glossary*", https://www.gartner.com/en/information-technology/glossary

Heieh T and Simonson A, (2003), "*Energy Risk - A Refined Approach for Assessing Liquidity Risk in US Energy Trading Operations*", http://www.riskcenter.com

Investopedia, (2021), "*Investopedia Dictionary*", https://www.investopedia.com/financial-term-dictionary-4769738

ISO 31000, (2018), "*ISO 31000-2018 Risk Management – Guidelines*", https://www.iso.org/standard/65694.html

National Institute of Standards and Technology, (2021), *"Computer Security Resource Center (CSRC) Glossary"*, https://csrc.nist.gov/glossary

Risk.Net.com, (2021), *"Risk.Net Risk Glossary",* https://www.risk.net/glossary

Technopedia, (2021), "*Technopedia Dictionary*", https://www.techopedia.com/dictionary

US Energy Information Agency, (2020), "*EIA Glossary*", https://www.eia.gov/tools/glossary/

Wikipedia, (2010), "*PnL Explained",* https://en.wikipedia.org/wiki/PnL_Explained,