The Integrated Knowledge Stack™

Abstract:

Organizations continuously struggle with how to better control their ever-changing operational environment, which is digitizing at the rate of a bullet train, while trying to automate and scale to keep up with customer, competitive, and market demands to stay current, and in a leadership position. This speed of change and loss of transparency and traceability has resulted in fractional knowledge. Instead of comprehensive traceability across technical, functional, and operational categories of knowledge, decision makers have myopic views resulting in high-risk decisions.

With Digital Transformation (DX) and Operational Risk Management initiatives used to address change to meet market and competitive challenges, it is imperative to have both comprehensive and perpetual knowledge.

Unfortunately, fractional knowledge, which is delivered today, has created an untenable barrier, including limiting Knowledge sharing between stakeholders that is required for data driven decisioning. This barrier must be removed so that decision makers have the information and knowledge that allows them to work cooperatively and regain control.

This paper presents a new framework to organize and structure Technical, Functional and Operational categories of Knowledge broken further down into 7 layers that reside in business/mission software today. It further discusses the current expectation of knowledge versus what is actually needed in support of DX and Operational Risk Management activities while touching on some of the efficiencies in labor and cost that can result from appropriate extraction and application of the retrieved knowledge from software-driven operations. It also discusses how a comprehensive extraction can enable a data driven and successful digital transformation and operational risk outcomes in perpetuity.

The Current Situation:

Every major organization today is either planning or engaged in some level of Digital Transformation (DX) or Operational Risk Management. With so many organizations running legacy operations, competitive pressures and customer demands are significantly impacting their market position and ability to create broader value. These challenges have also accelerated the need for speed, agility and improved effectiveness of operations. However, organizations are making decisions with limited understanding of the current state of their operations which, in turn has negative effect on how operational risk is currently managed. Agility and speed, key objectives to satisfy today's market needs, require a data-driven understanding of the current state (legacy and/or modern operations), to reach target organizational goals.

To put this in perspective, Digital transformation (DX) investment is expected to reach $1.3T worldwide and $433B in the US, in 2021. Approximately 70% of the DX investment, ($900B) is "wasted", in large part *due to cost and time delays caused by not-well-documented legacy operations* (IDC, PwC). Half the software applications [running business/mission operations] in organizations today are estimated to be custom, legacy code that is a major hindrance to successful digital transformation.

Digital transformation, to achieve operational effectiveness, includes activities such as legacy application modernization, application (and data) cloud migration, post M&A integration, and application portfolio rationalization. The complexity of DX includes understanding custom/packaged operational software, cloud/on-premise hybrid IT infrastructure and, of course, transparency of the operational state (current, transitional, and future) to keep pace with required changes.

Operational Risk is less transactional, nor is it project based. Operational risk management addresses change and evolution of regulation/compliance/audit measures, and provides data driven transparency of the flow of business/mission data across complex software applications. This is required in perpetuity.

Balancing the need for operational effectiveness and meeting requirements is a race in which most organizations are lagging, held back by the lack of transparency and limited traceability.

With many businesses having as much as 80-95% of operations running in software, transparency of operations has become a fundamental challenge. Software is not seen as an operational enabler, rather it is addressed as an "IT" element, with several discrete components, application by application, and always with a technology bias. This approach has increased risk and increased complexity within most organizations.

A large hurdle, for a number of decades, has been the tools available to extract and analyze the software to deliver this transparency/knowledge of current operations. Most tools, individually, are focused on a narrow field of technical or business views and do not provide comprehensive nor integrated operational knowledge (business process, data/term lineage and technical implementation). Manually extracting comprehensive operational knowledge is time consuming, error prone and very expensive. Frustrated, some organizations continue search for improved automated solutions, while most others heavily rely on system integrator/service providers to deliver results.

These integrators/service providers use a combination of existing myopic tools and a heavy labor component. The resulted is nearly always uncoordinated and uncorrelated results – with significant human extrapolation or assumption. This has usually resulted in stove piped, error prone, and fragmented knowledge. This fragmented knowledge doesn't come close to addressing operational effectiveness and it increases operational risk. Although decisions are still made by organizations with this fractional knowledge, the result is partial/narrowly scoped successes, expanding costs and complexity, and broadening operational risk due to knowledge gaps.

There is a Better Way:

Automate by delivering a repository of comprehensive static operational knowledge views and share this baseline throughout the organization for planning and executing transformations or measuring/evaluating operational risk. Project teams will have the transparency and traceability to successfully plan and execute operational changes. Operational Risk teams will have the transparency/traceability and data they need to evaluate against their internal risk models and manage risk closer to real-time. Automated assessment of the current state delivers value: comprehensive operational knowledge and the efficient extraction/expression of the layers of knowledge to build and deliver transparency, traceability, and correlation which are required to move forward.

There are three distinct categories of "Knowledge," and within each category, there are layers that further detail the elements of information retrievable from human- and software-run operations.

These three categories of knowledge and the layers within them are represented in Figure 1 below — Integrated Knowledge Stack™. These categories of knowledge are defined as follows:

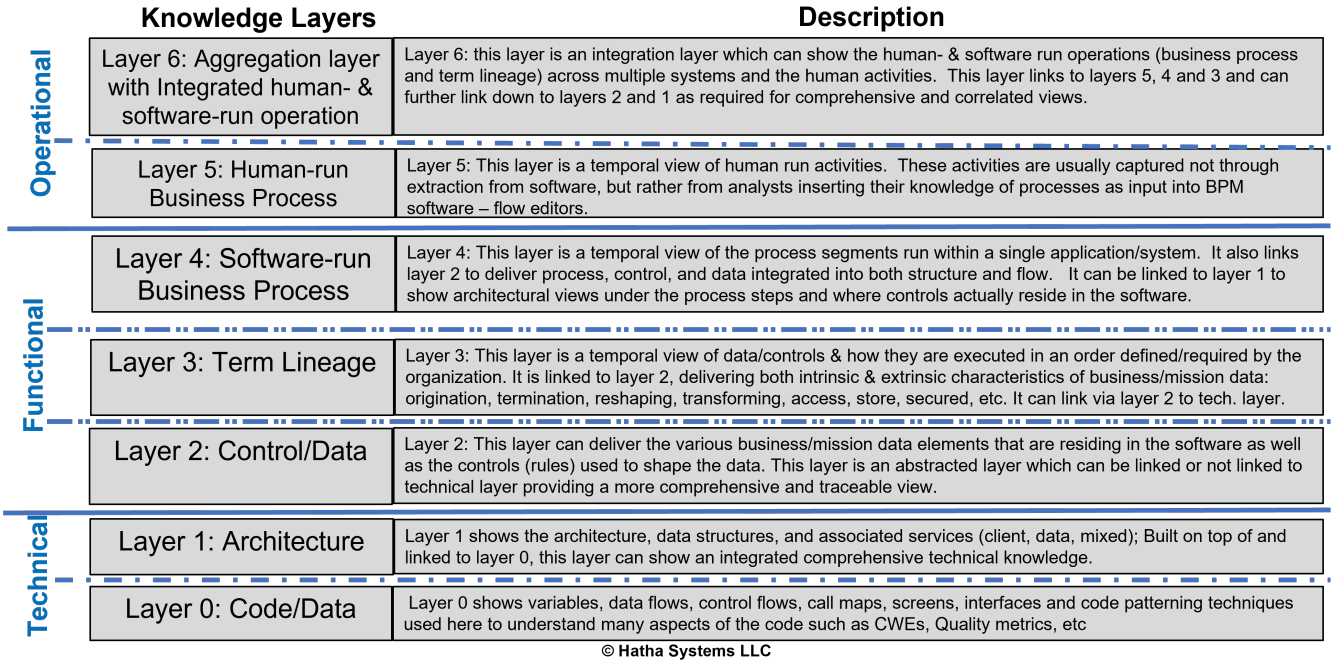
1) Operational knowledge is the information of how a business is run across a multitude of software applications and human activities. It consists of business transactions and business capabilities. It includes both human and software run process and data.

2) Functional knowledge is defined as business processes and data-based information residing in a single application. It represents process and term (data) lineage segments implemented within the application. The functional layer knowledge can be linked from one application to another, and human-run processes to provide operational layer views.

3) Technical knowledge is defined as the mechanisms within software that are used to build business process and data operations in a single application. This includes technical components such as structures, flows, and other artifacts that are the used to run software-based operations.

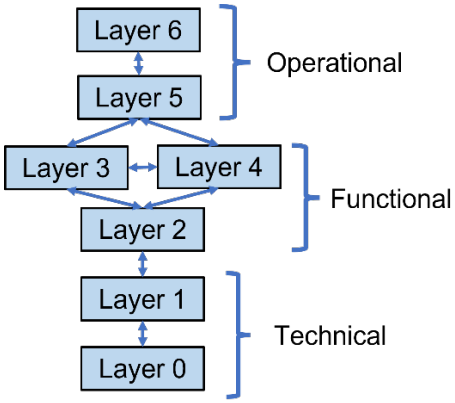
The layers within each category are further defined in Figure 1, linking extractable knowledge to obtain in-depth and in-breadth understanding of business/mission operations within an organization.

Figure 1: INTEGRATED KNOWLEDGE STACK™



The Knowledge Stack's seven layers of knowledge build on top of each other to deliver in-breadth and in-depth understanding. Figure 2 demonstrates the linkages and interactions which can be discovered and viewed with proper tools.

Figure 2: INTERLINKED KNOWLEDGE across the Knowledge Stack



The layers of the Knowledge Stack provide a comprehensive operational view and understanding. This knowledge can be collected in several ways:

- **Manual analysis** is based on existing documentation and interviews with stakeholders and users, but it is slow and unreliable and heavily dependent on remaining SMEs if even available
- **Dynamic analysis** automatically captures information as an application runs
- **Static analysis** provides insight into the actual application code

Using static analysis, the layers can be inter-linked providing a more comprehensive view. Adding to this comprehensive view, custom attribution can be imported to provide an in-depth and in-breadth view with richness of context and the ability to traverse across the layers in a "Google-mapping" manner. Custom attribution can import human knowledge, specialized tools (CWE, CVE, Process mining, etc.) enabling static analysis to become a centralized knowledge repository.

It has yet to be proven whether comprehensive layered analysis can be achieved using dynamic analysis, traversing technical, functional, and operational layers. Integration across operational and functional layers may be achievable, although there are knowledge gaps. Technical layer analysis (in isolation) is delivered today by several vendors. Various dynamic analysis tools (e.g., execution software/process mining) can provide some operational and functional aspects, but do not combine with the technical layers and have knowledge gaps which are needed for this purpose. Dynamic Analysis is critical for operations run in packaged software where IP restrictions may not allow for customer access to sources.

Bringing static and dynamic analysis together should be a goal for every organization. Whether through custom attribution or manual inputs, bringing dynamic analysis knowledge into a centralized static analysis repository can add robustness and nuance to the operations as organizations become more sophisticated in the use of such knowledge.

Disclaimer: Any marking of the word Google is owned by Google Corporation.

Applying Knowledge:

Both DX and Operational Risk require the knowledge to be extracted across the knowledge stack. Static Analysis delivers the transparency required to support legacy application modernization, application cloud migration, post M&A integration/portfolio rationalization, Compliance, Audit, and Operational Resilience, as noted in Figure 3. Each of the DX activities require a combination of knowledge delivered across the various layers of the knowledge stack and are demonstrated in Figure 3, which also identifies some of the standards used to represent the knowledge and for sharing across analysis platforms.

FIGURE 3: DIGITAL TRANSFORMATION & OPERATIONAL RISK KNOWLEDGE REQUIREMENTS

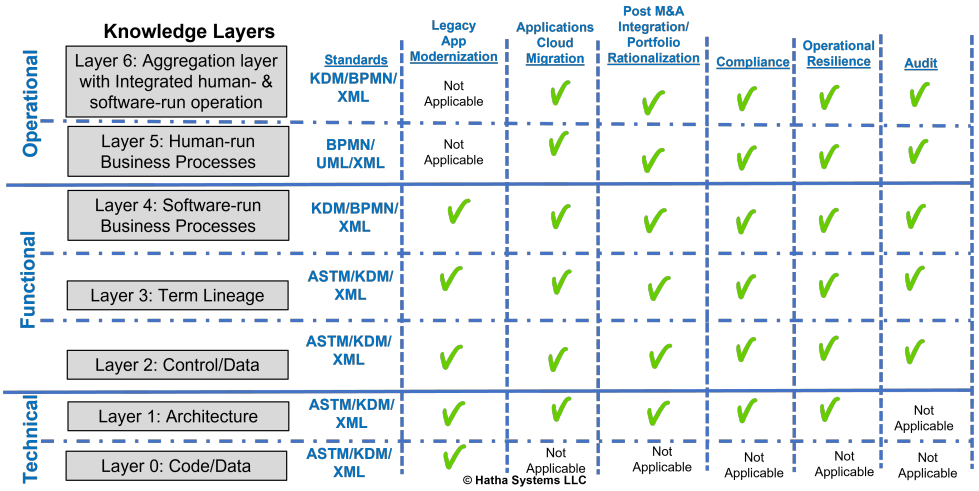
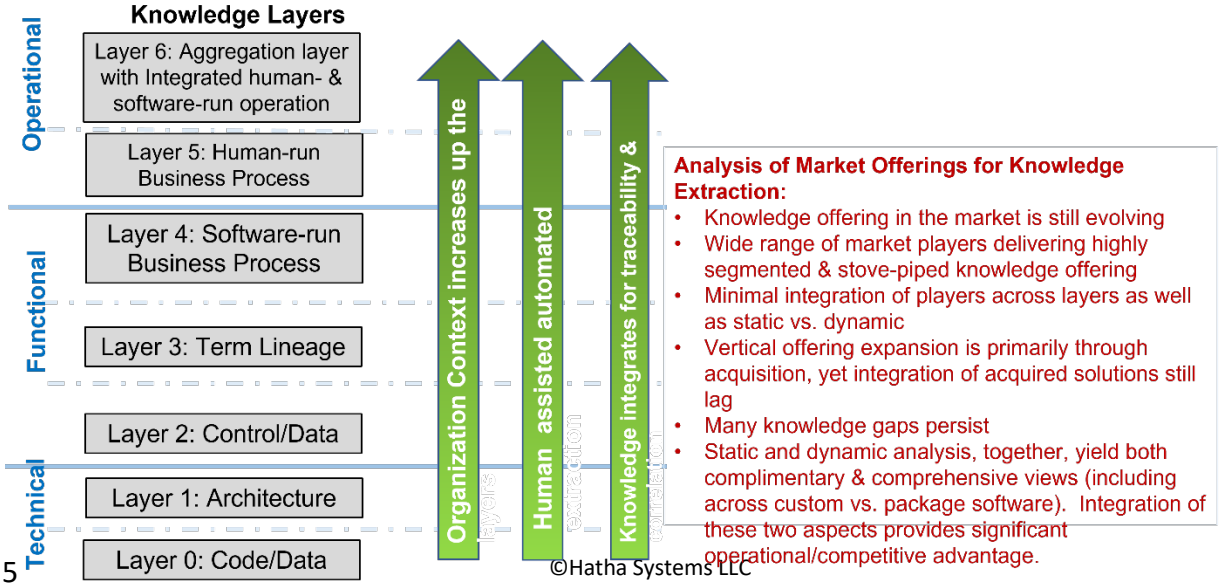


Figure 4, below, shows that the higher you go up the knowledge layers, the more context there is, requiring human assisted automation to steer extraction/analysis. However, the need for automation is even more critical due to the complexity of interdependencies and correlation not achievable with myopic and or manual efforts applied today. Automated cross-layer analysis delivers a more integrated and correlated result which, in turn, can provide a comprehensive view.

FIGURE 4: INTERACTION ACROSS KNOWLEDGE LAYERS



Figures 5 and 6 show the current state of knowledge expected vs. actual knowledge needed by the organizational stakeholder(s) to perform their tasks. Stakeholders are categorized based on industry norms as Dev Ops, Biz Ops, Risk Office, Chief Data Office. Currently, there are many vendors who participate in providing software analysis across one or two knowledge layers.

Additionally, most organizations have internal stakeholder stovepipes implementing fractional approaches, without the understanding of the value of integrated knowledge. This has resulted in continued implementation of fractional operations and in turn introducing operational risk. With a broader knowledge base, various DX and Operational Risk activities can be data driven to deliver required results. Additionally, the lifting of the unintended barriers changes how DX and Operational Risk can be more effectively implemented and managed. Knowledge can be securely centralized for viewing, analysis, and decision-making, enabling a cross functional team with more thorough information for more balanced, data driven planning and implementation.

FIGURE 5: CURRENT STAKEHOLDER KNOWLEDGE AVAILABLE

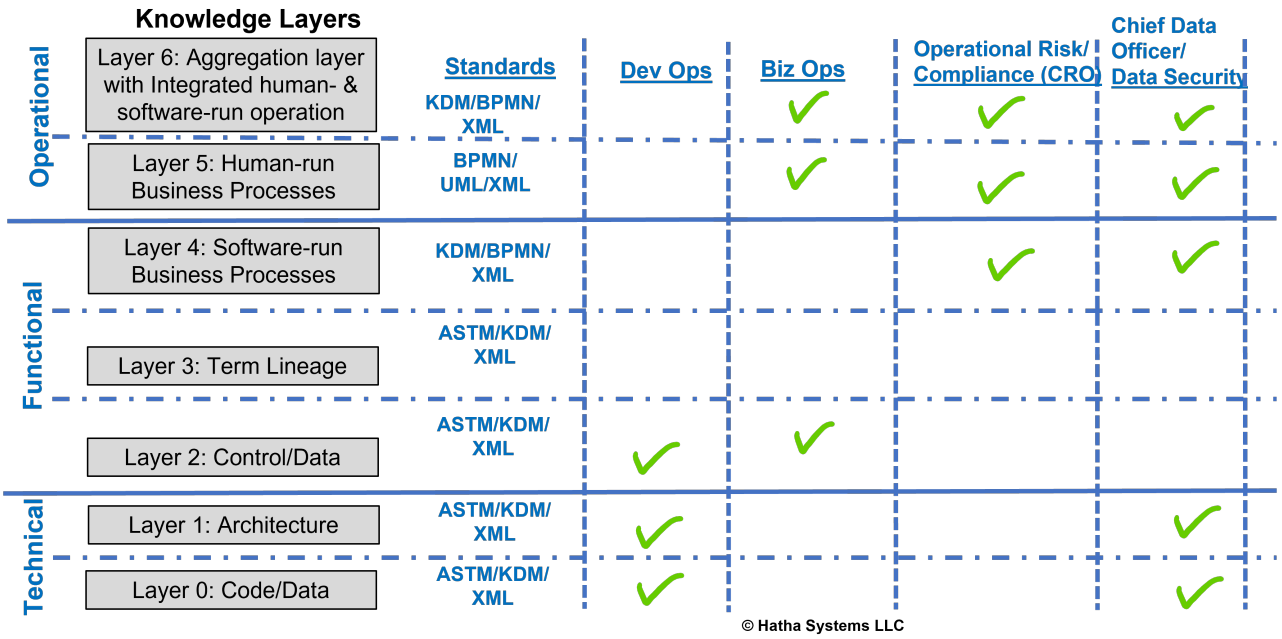


FIGURE 6: "SHOULD BE" STAKEHOLDER KNOWLEDGE REQUIREMENTS

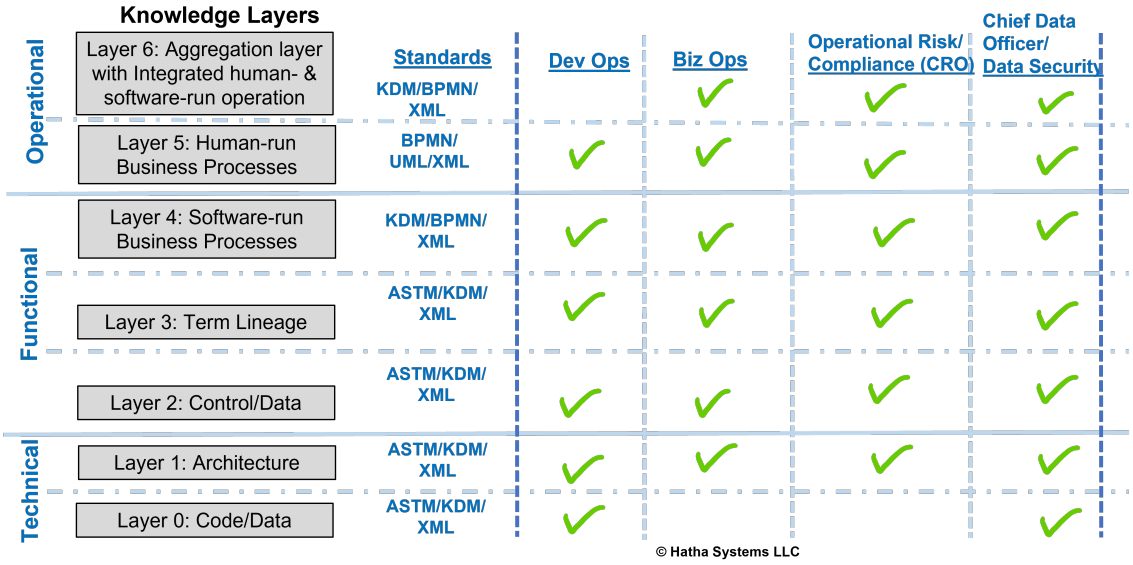
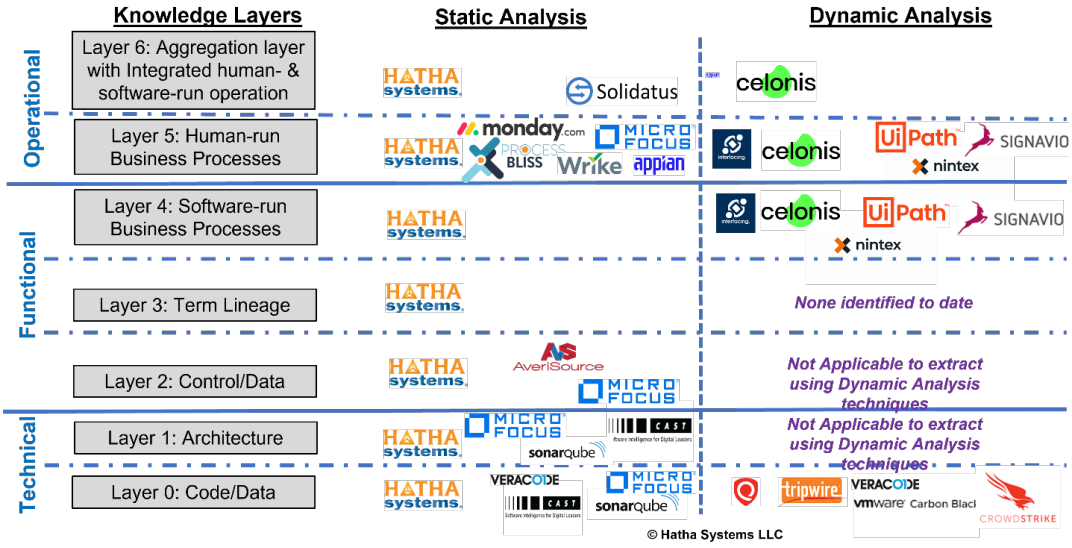


Figure 7, below, shows a sample set of vendors who deliver knowledge in the various layers. These vendors are primarily supplying discrete solutions with the vast majority of them delivering specialized technical knowledge. Static Analysis includes code weakness analysis, code quality analysis, and occasionally business rules extraction, business process extraction, term (data lineage) extraction. Dynamic analysis includes vulnerability analysis and process mining.

FIGURE 7: VENDOR LANDSCAPE



Note: Not all vendors are represented, and all data is obtained from public information. Please contact us if you see missing or misrepresented data or solutions.

Figure 7 shows the current state of knowledge delivered, by a wide sample of the vendor community, mapped across the Integrated Knowledge Stack™ framework. Granted, we have not included every vendor; we included a significant number who have both name recognition and brand awareness across markets and a few who may not.

Integrating the Knowledge:

When venders are positioned in the stack, it is clear to see that a comprehensive extraction and analysis requires an integrated approach to machining all layers of knowledge and interlinking them. What is discovered in Static Analysis is both different than and complimentary to what is discovered in Dynamic Analysis.

Static analysis properly implemented across the full stack, can result in the complete and granular mapping of the operational landscape — the process flows and associated rules, the underlying software mechanism running the **f**lows, and the business data/records/flows.

Bringing all these layers of knowledge together, using such advanced techniques as telescoping (in-depth/in-breadth) and version management delivers transparency of the current operational baseline in perpetuity. This is extremely important since organizations and their operations are constantly evolving. This "Google-mapping" of an organization's operations creates a current baseline or "ground truth", enabling data driven and traceable transformations and risk assessments.

Dynamic analysis, when properly implemented, cannot link all the layers in the stack. But the layers which can be integrated, deliver significant knowledge NOT available through static analysis. In the business process layer for example, tools can demonstrate the flow of process and data while they are executed capturing the actual activity. In addition, how the customer moves across the process flow while being executed is also traceable to understand customer behavior. Dynamic analysis cannot capture the granular detail nor all possible execution paths which are needed for traceability requirements in audit/compliance, resilience, and security, other '-ilities'.

Bridging the two (static and dynamic) analyses can be of significant value to digital transformation and operational risk management. Imagine if static analysis is "Google-mapping" operations, dynamic analysis is "traffic overlay on top of the Google map". When addressing operational risk, having both views enable resilience to be addressed with a more complete view … and impact.

Conclusion:

Operational transparency is critical to organizations as they continue to struggle to keep pace with market/competitive pressures and customer demands. This transparency available to organizations, in its current state, is fragmented at best, with significant gaps resulting in risky decisions for both Digital Transformation and Operational Risk activities.

Integrated Knowledge Stack™ defines, for the first time, a framework that enables a structured approach to extract knowledge and establish operational transparency. It defines a set of interlinked layers of knowledge which are implemented across the hybridized (human- and software-run) operational landscape of every organization. The Stack delivers, to organizations and tool vendors, an unprecedented opportunity to standardize on a common framework which can provide a cohesive, consistent, common approach to delivering the knowledge required to reduce risk and improve data driven decisioning.