Integrating Security and Risk Management into the Cognitive Enterprise

By William Ulrich

The rapid onset of enterprise-wide, artificial intelligence (AI)-based automation that promises increased efficiency, effectiveness, and customer satisfaction will bring along new challenges. The proliferation of autonomous technologies across a business ecosystem introduces new points of risk and greater potential for security breaches. Safeguards linked to one-off processes, controlled by one or two long-time employees, will be ripped away as automation sweeps through organizations and technology replaces human resources in ways yet unforeseen.

"Cognitive Enterprise: Envisioning the Business of the Future"[1] outlined the purpose and underlying concepts of the cognitive enterprise and highlighted steps toward achieving the cognitive enterprise vision. Whereas this white paper offers insights into how the cognitive enterprise can proactively protect itself from risks and security incursions by building business-driven safeguards into its underlying DNA.

Defining the Cognitive Enterprise

The "cognitive enterprise" describes a business that learns, adapts, and scales on an evolutionary basis, rooted in a deep and expansive understanding of the business ecosystem in which it operates. The cognitive enterprise is highly efficient, highly effective, and maintains excellent levels of customer satisfaction. Efficiencies are gained through dramatically increased levels of stakeholder and capability automation. Effectiveness, on the other hand, is delivered through dramatically improved strategy execution, enhanced learning, and adaptability. Collectively, efficiency and effectiveness improvements lead to improved customer satisfaction.

As organizations move up the cognitive maturity scale, human-led and human-assisted tasks increasingly become machine-assisted and ultimately machine-led tasks. As automation takes over more stakeholder roles, organizations must establish foundational capabilities to propagate risk and security related measures across their respective business ecosystems.

Defining and Integrating Risk and Security Perspectives

Risk management and the ability to provide security against those risks should be top priorities for public and private sector organizations across the globe. To achieve these risk and security safeguards, organizations must establish a common understanding of risk and security within their business ecosystem, as well as where risks and security intrusions manifest, and how they can be proactively addressed.

Risk is defined as a situation involving exposure to danger or loss, and further represents a perspective on the possibility of encountering danger or experiencing loss. Risk-related categories include strategic, compliance, operational, financial, and reputational risk. Violations of industry regulations, financial practices, and legal statutes are just one manifestation of where risk management is tested on a regular basis. Beyond these simple categorizations, risk is situational and context dependent. Assessing risk requires assigning levels of risk or risk ratings framed by specific business context.

Security is defined as a state of being free from danger or threat. Security is addressed in multiple ways across a business ecosystem and, like risk, is similarly context dependent. Security protects from threats and vulnerabilities as it pertains to every aspect of a business ecosystem. In the cognitive enterprise, security-related capabilities authenticate and authorize sentient actors, constrain or allow access, and play other roles based on the real-world objects being secured.

Unwanted or prohibited access by external or internal actors is one focal point of security. In this category, organizations seek to authenticate and assign authorization rights to human and machine-based actors. These actors often seek access to organizational assets, products, facilities, markets, customers, partners, and a wide range of other business objects. Organizations additionally create access-related constraints on these same business objects, which can range from preventing the viewing of certain agreements or intellectual property to preventing access to facilities, products, assets, or even markets.

Security and risk management are inextricably linked perspectives. Risk management provides insights into the potential for loss, damage, or destruction that can result from a threat that exploits a vulnerability. Security management seeks to protect an organization from those threats. Corresponding investments in security for a given business object reflect the degree of risk associated with that object in the context of a wide range of business scenarios. For example, a highly sensitive facility with a high degree of threat exposure warrants a magnified security focus. Capabilities must be in place to assess potential risk exposures and provide corresponding security across all applicable business objects for a variety of business scenarios.

Cognitive Enterprise's Dual Foundation Establishes Risk and Security Management Baseline

The cognitive enterprise has a built-in apparatus to deal with global risk management and security demands. As the vehicle for addressing risk, security, and numerous other considerations, the cognitive enterprise is built upon the dual foundation of a business knowledgebase and cognitive computing, the latter of which incorporates a cross-section of AI and related technologies. Figure 1 highlights these dual-foundational perspectives along with a very small sampling of cognitive enterprise business scenarios.

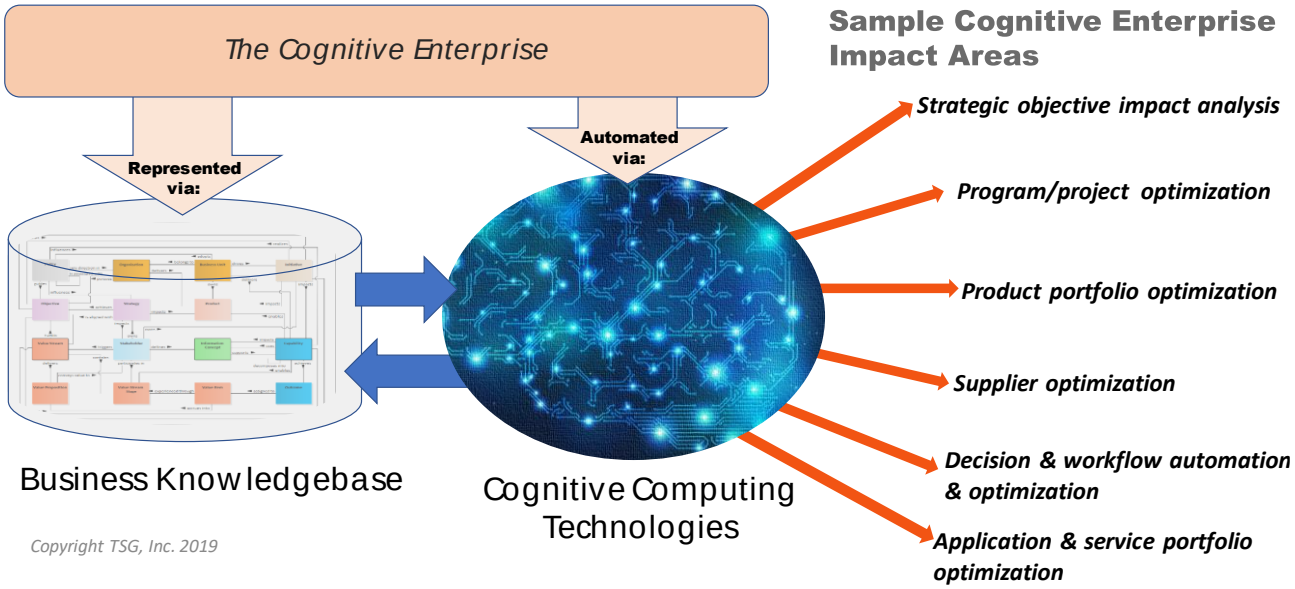


Figure 1: The Business Knowledgebase and the Role of Cognitive Computing

The business knowledgebase represents a formal, principled mapping of an organization's business ecosystem, based on the principles and practices defined by business architecture.[2] The business knowledgebase contains a fixed vocabulary defining a rationalized set of business objects with a finite set of defined states, where actions are triggered by external and internal events, framed by end-to-end stakeholder value delivery. Specifically, encapsulating a holistic, rationalized, scalable, and cross-business-unit perspective of an organization in a knowledgebase provides ecosystem-wide transparency and scalability based on a formally captured, highly rationalized understanding of the organization. Specifically, the knowledgebase provides total transparency to critical points of exposure where organizations may selectively apply risk related controls and security related constraints.

Cognitive computing provides the underlying "engine" that, when coupled with the business knowledgebase, serves as the technology enabler behind the evolution of the cognitive enterprise. Cognitive computing is not one type of technology but rather incorporates multiple technology categories that include AI, deep learning, neural networks, natural language processing, rule-based machine learning, finite state machines, predictive analytics, and quantum computing.[3] These technologies will continue to evolve in alignment with the evolution of the cognitive enterprise. But suffice it to say, enough cognitive computing power and technology are available today to move organizations toward the cognitive enterprise vision.

Envisioning the Cognitive Enterprise from a Security and Risk Perspective

The cognitive enterprise requires formal, shared clarity of essential aspects of an organization in order to establish, interpret, validate, deploy, and enforce risk management and security-related constraints across the business ecosystem. This degree of clarity is housed in the business knowledgebase.

When these business objects are coupled with certain actions, they manifest in the form of "capabilities." For example, a capability called Channel Activation represents all actions related to activating the "channel" business object. Each business object requires a corresponding set of risk and security related capabilities that provide the formal foundation for ubiquitous risk and security enablement. Consider the following scenarios within a cognitive enterprise and its risk-related focal points:

- Customer engagement in one business unit is rapidly reflected and integrated for that customer across all business units, regions, and product lines. In this scenario:
  - Customer risk is automatically evaluated based on an aggregated perspective of that customer across business units, which includes risk associated with past actions, agreements, claims, location, and history.
  - Customer security access is automatically set to an authorization level commensurate with the degree of risk presented by that customer and adjusted in real time.
- A virtual product manager conceptualizes and designs new products while automatically considering related products with similar capabilities, reframing the product portfolio in the process. In this scenario:
  - Product risks are established based on related or similar products and related risks within the portfolio.
  - Product risks are derived based on the risks associated with the entitlement-enabling capabilities that make possible the delivery of services defined by that product.
  - Product security access is established based on related product risks and other risk considerations associated with markets, customer categories, and policies.
- A virtual program manager leverages a comprehensive understanding of proposed and inflight projects to identify cross-project impacts and conflicts and produce an optimized program and project portfolio that are sequenced by strategic priorities and interdependencies. In this scenario:
  - Project risk assessments are determined and incorporated into project and program planning based on the assets, location, participants, and other business perspectives involved in the project.
  - Project security is established based on associated restrictions associated with the business object and business unit driving the project.

These scenarios highlight the cross-organizational, rapid assessment, and actions taken, particularly by the virtual or automated program management stakeholders. When risk- and security-related capabilities are engaged as automated capabilities, based on the cross-organizational perspective represented in the

business knowledgebase, risk and security are not afterthoughts but rather integrated aspects of every action taken across an enterprise. A highly functioning cognitive enterprise would engage rule-based machine learnings to ensure that each interaction moves the organization up the risk and security maturity curve.

Security and Risk: Defined in the Business Knowledgebase

The business knowledgebase, leveraging formal business architecture mapping principles, defines the business objects targeted by risk- and security-management capabilities. The knowledgebase further defines the information related to each business object, as well as how the capabilities enable value delivery. The knowledgebase is also used to associate risk- and security-related capabilities to current-state and future-state technology deployments, including future-state software services, enabled under a cognitive computing environment.

The perspective on risk and security within a business architecture capability map has historically been too high-level and too vague to be actionable. First- and second-generation capability maps contained Level 1 capabilities called Security Management and Risk Management. This positioning was often taken to raise the visibility of risk and security with management who wanted to see these topics at the top of the capability map. While the approach made for a nice picture, it also resulted in making security and risk management unactionable from a capability perspective.

This historic approach removed all context from an organization's ability to manage risk and security. Not all risk and security are equal, and not all risk- and security-related capabilities are the same. For example, a Facility Access Management capability differs from network, patient, operation, route, product, and other types of security access management capabilities. Similarly, an Agreement Risk Management capability differs considerably from location, asset, partner, order, and numerous other risk-related capabilities. Each set of capabilities is unique and specialized, based on the objects targeted for risk determination and the objects being secured or being secured against.

Establishing Targeted Risk Management Capabilities

Weaving security management and risk management into the fabric of a business ecosystem requires applying risk- and security-related capabilities in specific contexts. Context requires breaking down what is meant by risk and security and associating related actions with specific business objects in meaningful ways. In order to achieve this context, risk- and security-related capabilities are associated with business objects and actions; these objects/actions become capabilities under a given Level 1 capability.

Consider the example shown in figure 2, where the level 2 capability under the level 1 Agreement Management (not shown) is called Agreement Risk Management. Capabilities decompose into levels to achieve greater granularity of purpose. Three level 3 capabilities provide greater granularity on Agreement Risk Management. These lower-level capabilities assess the level of risk, set risk thresholds, and aggregate related risk perspectives based on available information. This last capability would consider agreement-related customers, partners, products, locations, and terms as a basis for assessing overall agreement risk.

Level	Capability Name	Capability Definition
2	Agreement Risk Management	Ability to identify, evaluate, assess, aggregate, articulate, and incorporate various exposures to harm, danger, or loss associated with a given agreement or portfolio of agreements.
3	Agreement Risk Level Determination	Ability to identify and define the level of risk associated with an agreement.
3	Agreement Risk Threshold Determination	Ability to identify and define the level of acceptable risk associated with an agreement.

3	Agreement Risk Aggregation	Ability to consider a collective set of risk factors about an agreement and represent them from a rationalized perspective.

Figure 2: Agreement Risk Capabilities

The pattern shown in figure 2 repeats itself across other level 1 capabilities that target markets, locations, products, assets, networks, customers, partners, conveyors, routes, human resources, jobs, and the business itself. Risk related specificity provides actionable context to risk management across the enterprise. Another aspect of business architecture allows for organizations to assign or deploy capability "instances" as they are realized across a business ecosystem, where each instance of a capability may be assigned a specific behavior. This formal aspect of mapping capability instances and related behaviors provides insights into how risk related capabilities should be implemented.

Aggregating Risk Perspectives Using Capability and Information Maps

In order for risk management capabilities to be effective, the capabilities require certain information, which is represented in the business architecture information map. From a risk perspective, a capability may need to determine related risk settings for objects to which it is connected. Figure 3 depicts how Agreement Risk Aggregation considers and integrates agreement-related risks linked to the customer involved, location associated with the agreement, and channel employed. Information created by one set of capabilities (i.e., outcomes), as shown to the right, is used by the aggregation capability to the left.

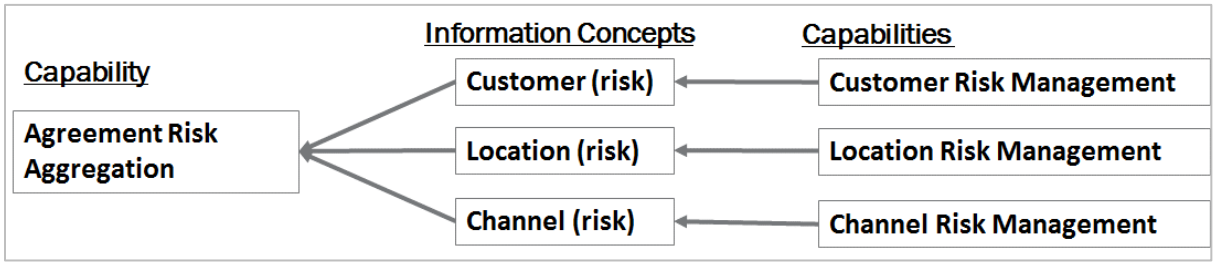


Figure 3: Agreement Risk Aggregation Leverages Risk-Related Information

Information concepts are an essential perspective defined within the business knowledgebase and correspond to the business objects defined within the capability map. These information perspectives provide formal insights to the data that would be used to power a cognitive computing environment where capabilities would be automated via means such as well-defined, highly reusable software services, a topic discussed later in this paper.

Multiple Perspectives on Security Management

Security management capabilities come in three flavors and include access-related security, security associated with sentient stakeholders, and information security, which has special considerations due to its widely employed nature. A discussion of, and examples for, each category follow.

Access-Related Security

The most basic level of security involves restricting or allowing access to real world objects. For example, access may be allowed or restricted to facilities, an asset, agreements, messages, or even a person, such as a patient. The types of access vary by business object and may include the ability to allow or restrict entrance into an object, viewing an object, or modifying an object. Figure 4 describes seven security related capabilities that control access to their respective business objects.

Facility Access Management Ability to establish, control, restrict, and administer rights to enter or use a facility in a variety of contexts.
Message Access Management Ability to restrict or allow the viewing or modification of a message.
Strategy Access Management Ability to control who, internally or externally, is able to view or modify a strategy.
Agreement Access Management Ability to define, control, authorize, grant, view, or modify an agreement.
Channel Access Management Ability to establish, control, and administer the level and extent of physical or virtual constraints associated with a channel.
Asset Access Management Ability to establish, control, restrict, and administer rights to view, use, or change an asset in a variety of contexts.
Market Access Management Ability to allow or restrict entry and participation in a given market.

Figure 4: Access Constraint-Related Capabilities

Note that the access management definition for a facility differs from those associated with a message, asset, or market, demonstrating how each of these capabilities is fit for purpose, making them actionable across a variety of business scenarios.

Security for Sentient Actors

Security management also considers constraining or authorizing sentient business objects, which include human resources, customers, partners, and assets. Sentient business objects represent actors who can take independent action, and these actors require additional security capabilities so they can be identified and authorized. For a cognitive enterprise in particular, it is critical to include intelligent assets in this category as they expand stakeholder automation across the ecosystem, which includes partners acting in various stakeholder roles.

The specific security capabilities involved fall into two categories: authentication and authorization. Authentication determines that the object is who or what it claims, while authorization assigns rights accordingly. Figure 5 highlights several capabilities that apply to sentient business objects.

Customer Authentication and Authorization Ability to verify customer identity and access rights and assign appropriate permissions to that customer.
Partner Authentication and Authorization Ability to verify partner identity and access rights and assign appropriate permissions to that partner.
Asset Authentication and Authorization Ability to determine the identity and accessibility levels of an intelligent asset, such as a robot or intelligent system of any kind, and assign appropriate permissions to that asset.
Human Resource Authentication and Authorization Ability to determine the identity and accessibility levels of a human resource and assign appropriate permissions to that human resource.

Figure 5: Authentication and Authorization Capabilities for Sentient Business Objects

The capabilities depicted in figure 5 would typically decompose into specific authentication capabilities and authorization capabilities. The criticality of authorizing access rights to assets, which ultimately may include a range of cognitive computing technologies, cannot be overstated. As automation infiltrates a cross-section of an enterprise, constraining assets becomes just as or even more critical than constraining human actors because cognitive computing assets can act more quickly and potentially do more damage.

Information-Related Security

Special security constraints are required for information. In the business knowledgebase, information represents the aggregate set of facts, statistics, attributes, and other types of data about an organization's business objects. Therefore, securing of information is managed through the aggregate, ecosystem-wide

perspective as defined under a level 1 Information Management capability. Figure 6 shows an example of commonly found information security capabilities.

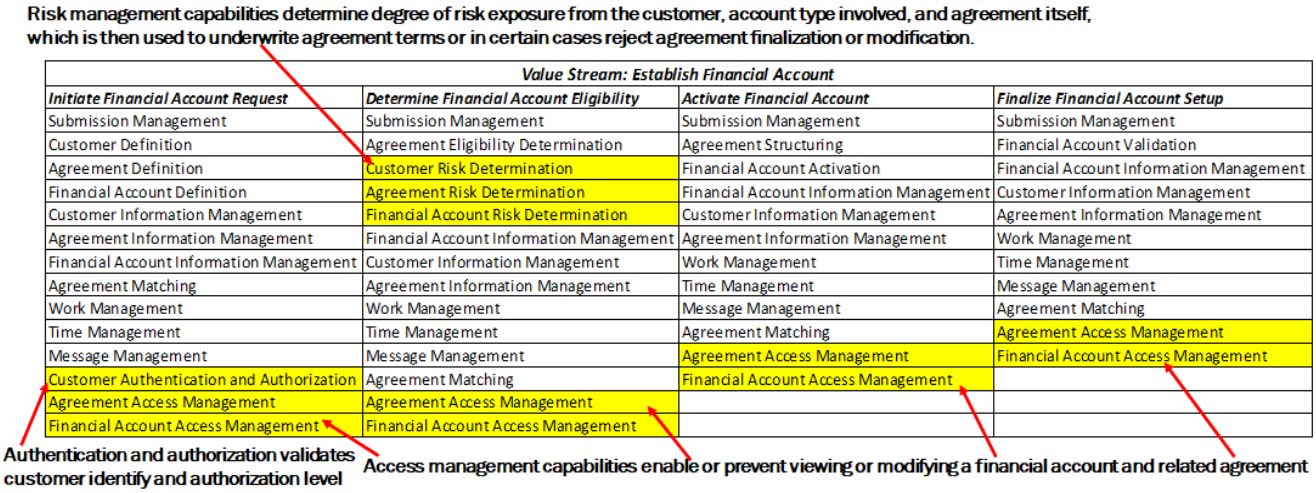
Information Security Management	Ability to control access, use, disclosure, disruption, modification, inspection, recording, or destruction of information.
Information Encryption	Ability to encode information in a cipher to prevent or limit its unauthorized access, change, or claim of provenance.
Information Obfuscation	Ability to conceal information content in a cipher using symmetric or public key encryption.
Information Non-Repudiation	Ability to ensure that information is from a known, determinate source using symmetric or public key encryption.
Information Security Level Identification	Ability to determine the degree of authority required to create, access, modify, and delete information.
Information Security Level Setting	Ability to establish authorization levels for particular information for types of persons or organizations.
Information Security Level Interpretation	Ability to interpret the degree of authority associated with a given point of access and allow or withdraw access based on the association between the degree of authority required and that of the accessor.
Information Access Control	Ability to allow or prevent individuals, organizations, and assets from viewing, using, modifying, or sharing information based on certain rules and defined authorizations of the accessing parties.
Information Access Constraints Definition	Ability to define and impose limitations of access rights to given information.
Information Access Constraints Interpretation	Ability to understand imposed access rights limitations for given information.
Information Access Enforcement	Ability to ensure that access rights are granted where constraints are not appropriate and to prevent access where constraints are in place to prevent access.

Figure 6: Information-Related Security Capabilities

Information-specific security capabilities include access controls but also include other concepts, such as encryption. This specialized set of security capabilities, which likewise benefits from formal automation, ensures that information has the requisite degrees of security just as an organization would secure its real-world objects.

Risk and Security Management in a Value Delivery Context

Placing risk and security management in context requires associating or mapping capabilities to the value streams they enable. Value streams represent an end-to-end perspective for a stakeholder or stakeholders to achieve a given value proposition. For example, if a customer wants to establish a new bank account, the value stream Establish Financial Account would be used, as shown in figure 7. Capabilities enable value streams as visualized through a technique shown in figure 7 called cross-mapping.



Value Stream: Establish Financial Account			
Initiate Financial Account Request	***Determine Financial Account Eligibility***	***Activate Financial Account***	***Finalize Financial Account Setup***
Submission Management	Submission Management	Submission Management	Submission Management
Customer Definition	Agreement Eligibility Determination	Agreement Structuring	Financial Account Validation
Agreement Definition	Customer Risk Determination	Financial Account Activation	Financial Account Information Management
Financial Account Definition	Agreement Risk Determination	Financial Account Information Management	Customer Information Management
Customer Information Management	Financial Account Risk Determination	Customer Information Management	Agreement Information Management
Agreement Information Management	Financial Account Information Management	Agreement Information Management	Work Management
Financial Account Information Management	Customer Information Management	Work Management	Time Management
Agreement Matching	Agreement Information Management	Time Management	Message Management
Work Management	Work Management	Message Management	Agreement Matching
Time Management	Time Management	Agreement Matching	Agreement Access Management
Message Management	Message Management	Agreement Access Management	Financial Account Access Management
Customer Authentication and Authorization	Agreement Matching	Financial Account Access Management	
Agreement Access Management	Agreement Access Management		
Financial Account Access Management	Financial Account Access Management		

Figure 7: Risk and Security Capabilities Enabling Financial Account Establishment

The value stream in figure 7 establishes the agreement and the financial account based on customer security levels and collectively determined risks, where risks are used to underwrite the agreement. Note that the highlighted risk and security capabilities apply to the customer, the agreement, and the financial account. When highly automated, cognitive technologies would be able to more efficiently and effectively surface and mitigate risks and impose security constraints beyond the capacity of the human resources and legacy technologies in place today.

Assessing Risk and Security Conformance Across a Business Ecosystem

Discrete, well-defined risk and security perspectives provide deep insights into compliance determination, investment or program analysis, merger and acquisition exposure, and any number of other business scenarios. The object-based capability and information definition protocol provides a formal perspective from which to determine current-state automations, amount of automation redundancy, or the lack of automation for a given risk or security management capability.

The technique for performing this analysis is called business-to-IT architecture cross-mapping. Figure 8 depicts the Agreement Risk Determination capability along with other capabilities under a level 2 capability called Agreement Structuring. The object-based capabilities are readily identifiable in software systems because they can be mapped to the use of that object either in the software itself or in the data structures the software references.

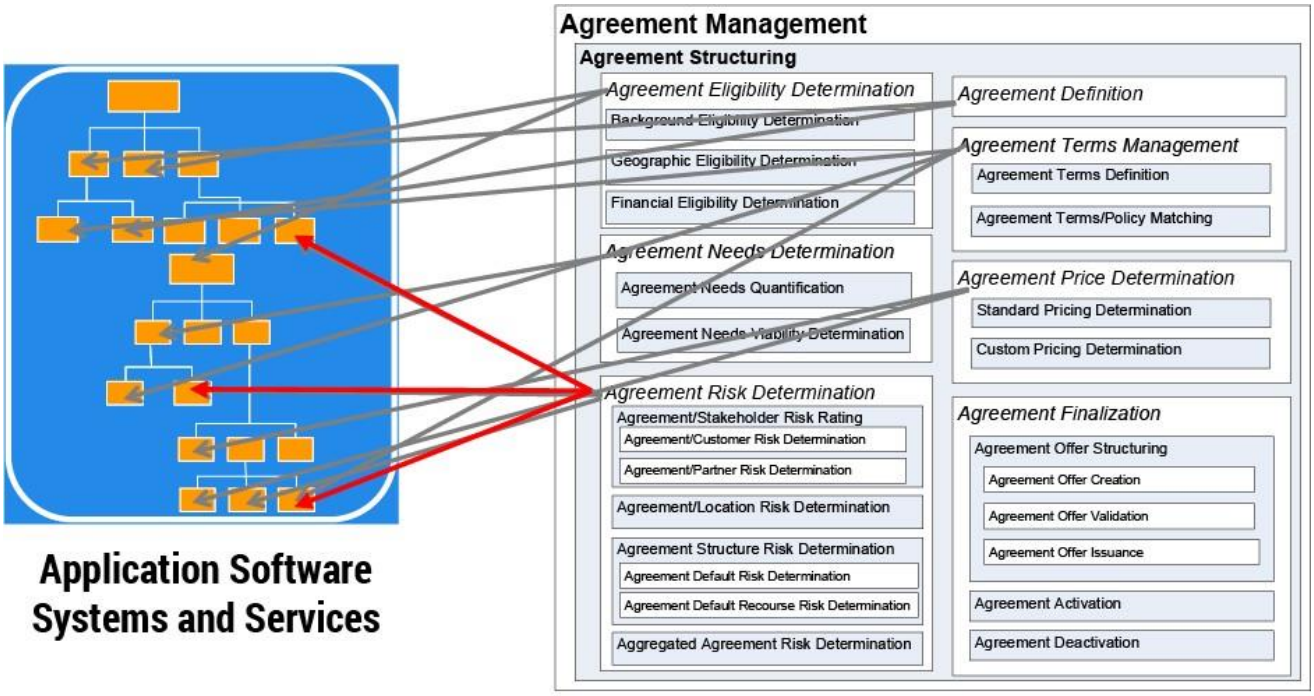


Figure 8: Cross-Mapping Risk and Related Capabilities to Application Systems and Software Services

Mapping risk and security capabilities to current-state systems demonstrates where and how well risk and security are being addressed or not being addressed in existing systems, providing insights into related system investments. Object-based focal points provide clarity of focus and scope missing from other business models such as business processes. Consider that business processes do not typically identify business objects and are therefore not decomposable based on bounded, nonredundant business perspectives. Consider, for example, the lack of reference to formal legal agreements often missing from business processes, in spite of the fact that agreement management is so central to the legal and practical viability of most organizations.

Standardizing Risk and Security Across a Business Ecosystem

One means of planning the design and deployment of cognitive computing technologies is to define discreet risk- and security-related software services that are uniquely defined and widely reusable. Capabilities establish essential business perspectives for creating well-defined, well-bounded software services. Creating reusable software services to automate risk and security related capabilities ensures that consistent, reusable software services are deployed across the business ecosystem. In addition, framing software services through the lens of highly rationalized capabilities ensures that automation of risk management follows a well-defined, integrated architectural perspective.

Just as capabilities frame the context for software services, low level capabilities similarly frame the context for microservices. Figure 9 depicts how risk management capabilities and related information concepts are used to frame the scope of corresponding microservices, with the goal being to ensure that microservices are well aligned to business-driven risk management requirements. As microservices are deployed, the relationships among capabilities, existing software deployments, and the newly deployed services are updated in the business knowledgebase. Microservices are merely one implementation perspective; the knowledgebase supports any number of other software design techniques and approaches.

Figure 9: Leveraging Capabilities to Define Microservices

Another consideration illustrated in Figure 9 is that capability use and management of information concepts further provide a clear perspective on data-related impacts. The connection to information concepts provides input to data design strategies for the future-state cognitive computing environment.

Risk and Security Guardrails in the Cognitive Enterprise

Effective management of risk and security is highly critical for most organizations, yet the formality of defining and deploying these capabilities is often lacking. As organizations move at their own pace toward becoming cognitive enterprises, the need for incorporating formal risk and security checkpoints into the overall architecture of the enterprise grows significantly. Organizations that wait, allowing cognitive computing technologies to seep into their ecosystems with no boundaries or formal architectural perspectives, can be putting their organizations at great risk.

Organizations seeking to become cognitive enterprises and correspondingly ensure that risk and security considerations are given top priority should consider the following steps.

1. Prioritize risk- and security-related formalization and focus based on business demands.
2. Carve out specific areas where executives want to focus risk and security safeguards, ensuring that the organization employs a reusable baseline solution.
3. Ensure that the business architecture adequately frames a comprehensive, holistic perspective on risk and security management across all business objects and related information perspectives.
4. Leverage formal business architecture principles to formalize the business architecture within the business knowledgebase.
5. Research and establish a plan to incrementally deploy cognitive computing technologies with a focus on deploying software services and microservices to deliver increasing automation of risk and security management.

Finally, risk- and security-related concerns must extend beyond risk management executives and security teams, particularly as cognitive computing is established in enterprises that are already overexposed in many cases to risks and security intrusions. The time to look at holistic risk and security demands is now, not after cognitive technologies gain a more entrenched foothold in your enterprise.

About the Author

William Ulrich *is President of TSG, Inc., Cofounder of the Business Architecture Guild®, and Partner at Business Architecture Associates. He is a thought leader in the field of business architecture and business and IT transformation. As a management consultant for more than 35 years, Mr. Ulrich serves as senior advisor, mentor, and workshop leader to corporations and government agencies worldwide. He may be contacted at wmmulrich@tsgconsultinginc.com.*

---

[1] The Cognitive Enterprise: Envisioning the Business of the Future, William Ulrich, 2019, www.tsgconsultinginc.com, http://nebula.wsimg.com/22adca13e4bf797369008e9e6ddd6693?AccessKeyId=83A5C131A46F2AE15F90&disposition=0&alloworigin=1.

[2] A Guide to the Business Architecture Body of Knowledge® (BIZBOK® Guide), Business Architecture Guild.

[3] The Cognitive Enterprise: Envisioning the Business of the Future, William Ulrich, 2019, www.tsgconsultinginc.com, http://nebula.wsimg.com/22adca13e4bf797369008e9e6ddd6693?AccessKeyId=83A5C131A46F2AE15F90&disposition=0&alloworigin=1.