Research Report

IBM's Unified Governance Framework (UGF) Initiative

Birgit Pfitzmann[1], Calvin Powers[2], Michael Waidner[3]

[1] IBM Research GmbH
Zurich Research Laboratory
8803 Rüschlikon
Switzerland

[2] IBM Software Group
IBM Raleigh (RTP)
Research Triangle Park, NC 27709-2195
USA

[3] IBM Software Group
IBM Somers
294 Route 100
Somers, NY 10589-0100
USA

IBM Research
Almaden · **Austin** · **Beijing** · **Delhi** · **Haifa** · **T.J. Watson** · **Tokyo** · **Zurich**

IBM's Unified Governance Framework (UGF) Initiative

Birgit Pfitzmann[1], Calvin Powers[2], Michael Waidner[2]

IBM Zurich Research Lab (1) and IBM Software Group (2)

Sept. 5, 2007

Abstract

Governance has become a huge topic in the business world. Key drivers are increasing regulatory pressure, needs for better risk management, and the desire of enterprises to monitor and influence their business performance faster. IBM's Unified Governance Framework is intended to cover the entire space of enterprise governance, with a focus on how IT-related services and components can support governance. We give an overview of the main parts of UGF, a governance lifecycle and a component model. We also show the use of UGF in devising consistent governance solutions by two concrete scenarios. The first scenario is a business-oriented one about the automation of business controls. The second scenario is primarily an IT-oriented one about access control, but shows how the strategic focus can help getting a broader view..

1 Introduction

Governance is currently a major concern in enterprises, getting high attention even from CEOs. There are three major drivers for this development:

- **Compliance** is arguably the strongest driver for better governance and for using IT (information technology) in governance solutions. The main reason is that many new laws concerning enterprises set new paradigms. While older laws simply stated that, e.g., accounting should be correct or the privacy of certain data should be preserved, new laws go much further: They typically require that the enterprise defines and documents processes to achieve the regulatory goals, that it shows this documentation to external auditors and possibly to regulators, that it regularly validates its processes, and that it documents all events that relate to the regulatory goals. The United States Sarbanes-Oxley Act is the best-known example of this new type of law. While these requirements are still technology-neutral, they go far towards requiring an overall enterprise governance solution that is both supported by IT, and extends into the governance of IT usage.

- **Risk management** is another driver. Partially, the recent increased interest in risk management is a consequence of compliance, because some regulations require well-defined risk management. However, risk management has always been part of business strategies, and with increasingly complex dependencies and fast changes both in the market and in underlying infrastructures like IT and electricity, there is a clear need to step up risk management also without regulatory pressure. In particular, operational risk has come much more to the forefront.

- **Business performance** in fast-changing environments also requires new governance structures. Most existing enterprise governance structures are actually geared towards business performance, not compliance or risk. This concerns aspects like strategy-making, planning, measurement of execution, and reward systems. Classically, most of this governance is done manually and at significant time intervals. With the increasing speed of market changes, the

increasing complexity of the enterprises and in particular their IT infrastructures, and the increasing availability of huge amounts of information in digital form, these governance processes have to be redesigned. Again, there is a need both for more IT support for the overall governance processes and for extending the business-level governance into governance of IT usage.

We find major aspects of governance well captured by the following definition from the OECD Principles of Corporate Governance [OECD_2004]; we emphasize them by italics:

"Corporate governance is the system by which business corporations are *directed* and *controlled*. The corporate governance structure specifies the *distribution of rights and responsibilities* among different participants in the corporation, such as, the board, managers, shareholders and other stakeholders, and spells out the *rules and procedures for making decisions* on corporate affairs. By doing this, it also provides the structure through which the company *objectives* are set, and the means of attaining those objectives and *monitoring performance*."

Following [ITGI_03], one nowadays distinguishes corporate governance, enterprise governance, and IT governance as the main governance types in the business world. Corporate governance mainly means governance at the highest levels of an enterprise and the balance with external stakeholders, in particular shareholders. IT governance means governance *of* the IT usage in the enterprise. Enterprise governance means governing all aspects of an enterprise at all organizational levels; it comprises corporate governance and IT governance.

Our goal with the IBM Unified Governance Framework (UGF) is to aid enterprises in implementing consistent enterprise governance, with a certain focus on the use of IT and IT-based services to achieve enterprise governance. For clarity, Figure 1 shows the two dimensions of IT in enterprise governance.
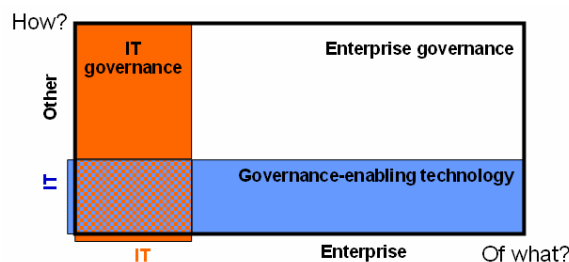

Figure 1   The two dimensions of IT in enterprise governance

While there are a number of governance frameworks, there are very few for the entire space of enterprise governance before UGF. The main purpose and novelty of UGF is to serve as a framework also for the governance-enabling technology for the overall enterprise governance space.

2 UGF Component Model Overview and Lifecycle

The core parts of UGF are a component model and a lifecycle. The component model is structured in layers. We start with the layers and the lifecycle, then survey the component model, and then present more details about the components.

2.1 UGF Layers and Lifecycle

Figure 2 shows the layers that we use for the UGF component model.

Figure 2　　　　*UGF layers (inherited from IBM's CBM initiative)*

The inner three layers are those of an enterprise, while the outer (red) layers represent the environment. The names used are consistent with IBM's generic Component Business Model (CBM) [CBM_07]. The strategy layer, also called directing, corresponds to the business strategy in the usual business sense, and the upper environment corresponds to the business environment as considered by the enterprise strategy. The tactics layer, also called controlling, corresponds to lower-level business planning. Specifically for the IT part of the enterprise, it corresponds to modeling (design), development, and deployment, as shown by the three sublayers. These terms can also be used in a more general contexts, e.g., for deploying an employee to perform a task. The lowest layer of the enterprise is the operations or executing layer. Here all normal business actions happen, as well as all IT runtime support, e.g., workflow execution engines.

2.2 UGF Lifecycle

A dynamic UGF view at a similar degree of abstraction is the lifecycle Figure 3. It can be mapped to enterprise governance as in the UGF component model, as well as to smaller scopes such as IT governance or data governance, or to completely different governance scopes like politics.
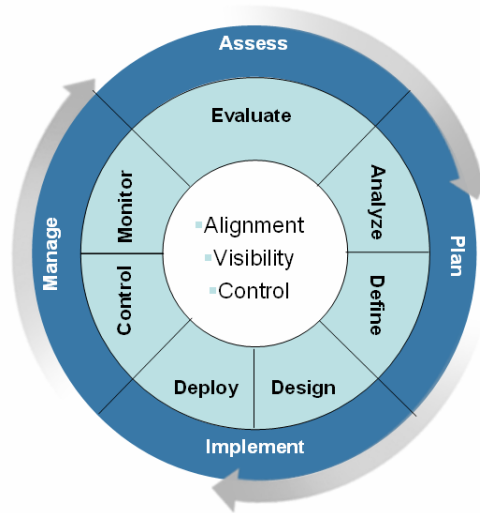
Figure 3   *UGF lifecycle*

2.3 UGF Component Overview

The core of UGF are the highest-level components, which we show in Figure 4. A component model, in IBM's terms, is a grouping of related functions and capabilities into components that communicate over relatively well-defined interfaces. A component can contain organizational structures, processes, people, and technology. The specific purpose of UGF is to focus on enterprise governance, i.e., to distinguish and describe governance components in more depth than the rest of the enterprise. Furthermore, UGF is cross-layer, while some other component models focus on one layer, e.g., the strategy layer alone or run-time IT architectures alone. While it would be too strict a goal that all enterprises restructure their governance precisely according to the UGF components, UGF should become the basis to show up gaps or unnecessary complexities in enterprise governance systems. Furthermore, it shows how different IT components can interact towards overall governance goals. So far, we found UGF to play this role very well in scenario and technology discussions.
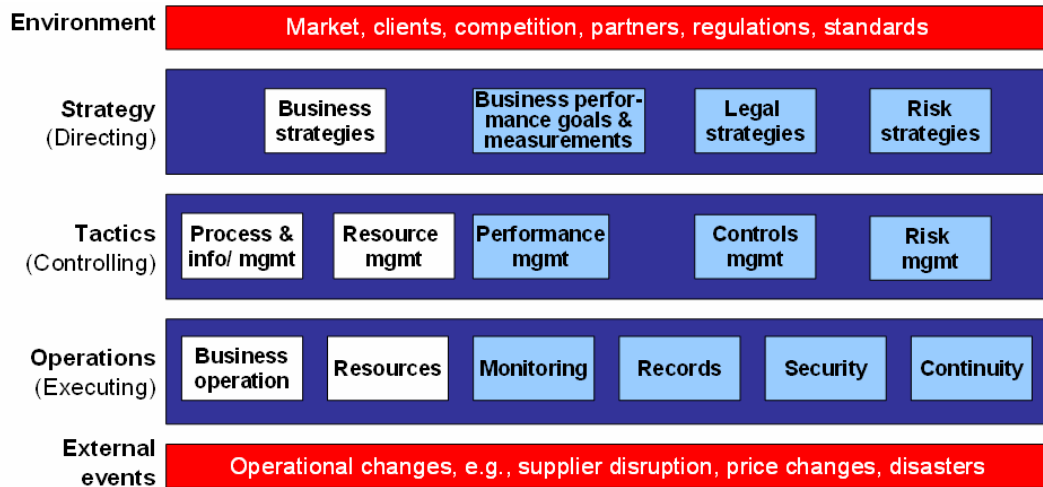
Figure 4   *UGF component model. The light blue components (on the right) are specific to governance; the white components summarize the normal enterprise activities being governed.*

We now briefly sketch the components; they are described in more detail in Sections 3.1 to 3.3.

- On the strategy layer, we summarize the normal enterprise capabilities as a component "business strategies". Governance deals with three main aspects: business performance goals, legal issues, and risk. On the strategy layer, this involves overall analysis, goal setting, and establishment of appropriate organizational structures. We therefore call the components "business performance goals and measurements", "legal strategies" and "risk strategies". These components depend on the overall business strategies, and sometimes modify them.

- On the tactics layer, we summarize the normal enterprise capabilities in two components: "Process and information management" and "resource management". The former corresponds to business parts organized by lines of business and business processes, the latter to functional units like IT, HR (human resources), and facilities. The governance capabilities on the tactics layer are designed at the same degree of detail as the normal capabilities, e.g., down to concrete business process steps or HR databases. Roughly, each of the components "performance management", "controls management", and "risk management" correspond to the strategy component above it. However, controls management is driven not only by legal strategies, but also by performance goals and risk strategies.

- On the operations layer, we summarize the normal enterprise capabilities in a similar way as on the tactics layer: "Business operation" means all standard actions for executing a business, including automated and human business process steps as well as human collaborative activity. "Resources" contain capabilities related to running the functional units, such as IT operations and day-to-day HR tasks. The governance components on this layer have been organized functionally: "Monitoring" corresponds to measurement systems; they are increasingly implemented in the IT support systems for business and resource operation. "Records" refers to record keeping, archiving, and retention; this is particularly important for audits. "Security" nowadays mostly concerns IT security, but there is also physical security. "Continuity" refers to emergency and disaster-recovery planning, high-availability measures etc.

2.4 UGF Information Flow Summary

The following two figures summarize the information flow between the different UGF layers. The arrows are roughly ordered according to the main components that produce and consume the information. Figure 5 shows the downward flows.
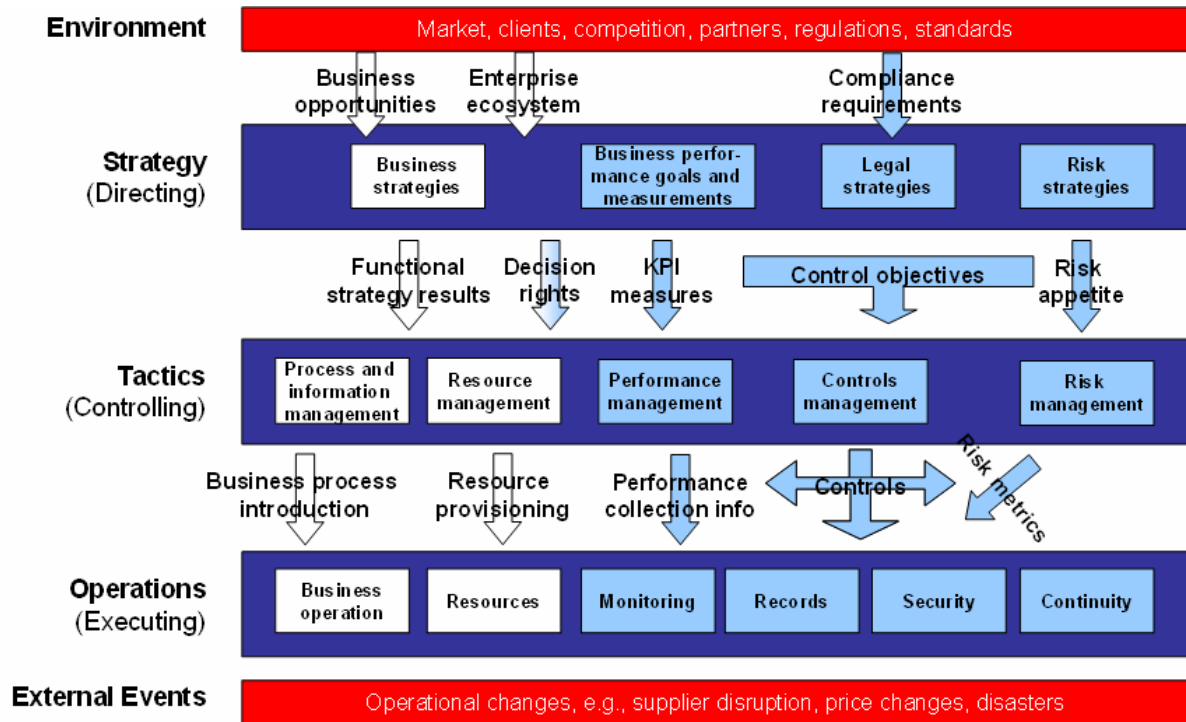

Figure 5   *Downward information flow between the UGF layers*

- At the top there are flows from the environment into the strategy layer. The normal (white) information is the business opportunities and enterprise ecosystem. They influence the business strategies and business performance goals. The main additional governance input is external compliance requirements, in particular laws and regulations, but also important standards and customer expectations.

- Between the strategy layer and the tactics layer, we summarize the results of the business strategies, as they are communicated to the normal tactics components, as "functional strategy results". Decision rights are a separate arrow in white-blue because they are an important result of normal business strategies already, but become even more important for governance (recall the OECD definition in Section 1), and they are strongly influenced by the governance-specific (blue) strategy components. The main information communicated from the setting of business performance goals and measurements is called KPI measures; KPI means key performance indicators. Control objectives are a core output from the legal strategies, but also arise from performance and risk strategies. The main output of the risk strategies is called risk appetite; it tells in broad terms how willing the enterprise is to take risk in different areas, and how it avoids or mitigates other risks.

- From the tactics to the operations layer, we show two normal information flows: Bringing business-oriented design decisions into practice is summarized as "business process

introduction"; this includes introducing corresponding information systems and human education. Information from the resource management to operations on resources is called "resource provisioning". Performance management mainly produces information about performance metrics to be collected, but indirectly (via horizontal arrows, which are not shown here) also influences in particular the resource provisioning. Controls management mainly produces concrete controls. Those are distributed almost throughout the enterprise (as everyone involved in audits or a Sarbanes-Oxley process will know), in particular into the process and information management within the tactics layer. However, important controls also go to the governance-specific infrastructures on the operations layer, i.e., monitoring, records management, security, and continuity, often in the form of policies.

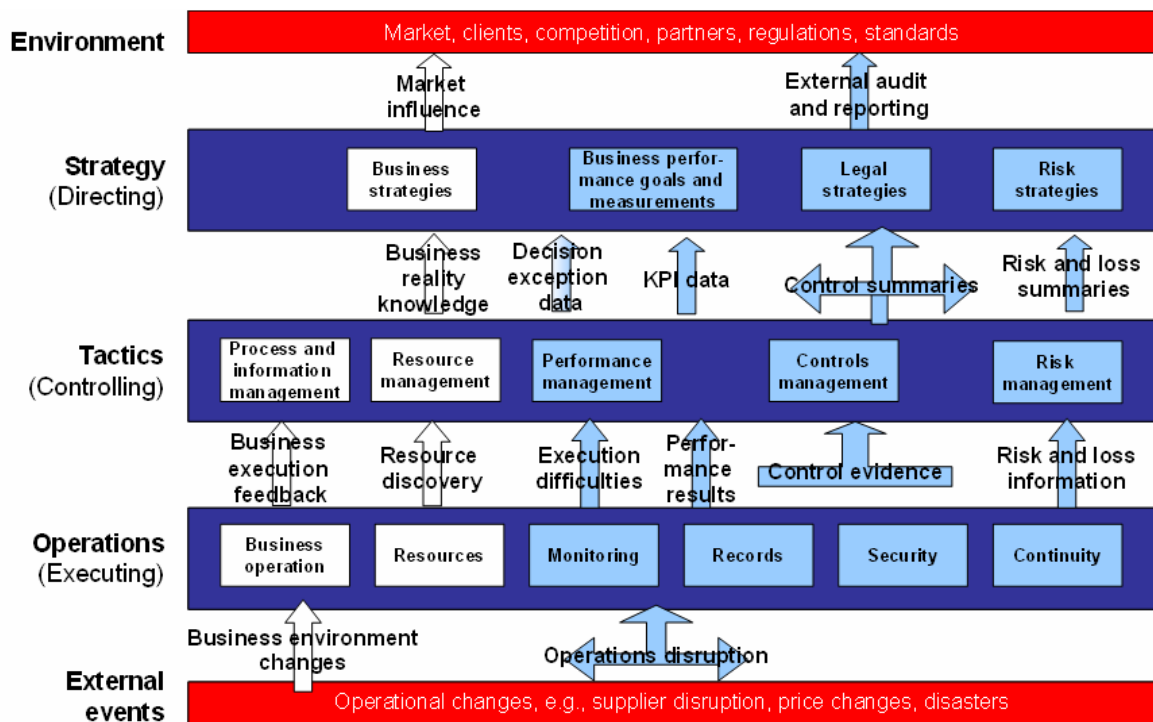Figure 6 shows the upward information flow.

Figure 6   *Upward information flow between the UGF layers*

- At the bottom, we have external events that are sensed at the operations layer. We distinguish the main ones into business environment changes and operations disruptions. The distinction between these events and the information from the environment into the strategy layer is not fixed; with increasing real-time processing more and more information will be monitored and analyzed by operations system first.

- From the operations layer to the tactics layer, we mainly see feedback at the level of detail where tactics goals were set. This is normal business execution feedback, execution difficulties and performance results mainly detected by the monitoring component, control evidence from all components that got controls, and risk and loss information (also often via monitoring). Furthermore, there is more static upflow about the real situation on the operations layer, at least

as long as not everything happening here is fully planned in advance; resource discovery (e.g., IT systems scanning) is shown here.

- The main information from the tactics to the strategy layer is aggregated measurements, i.e., the tactics layer evaluates low-level information into meaningful strategic summaries. The best-known such data are the measured KPI data. Control results are mostly statistics of passed and failed controls, but also KCI data belong here. Similarly, risk and loss summaries, including KRI data, are communicated. Decision exception data correspond to feedback about the decision rights and about internal standards. Business reality knowledge summarizes information that the strategy layer gets, in pull and push models, outside the pre-planned standard summaries and indicators.

- The strategy layer also informs the environment, e.g., by telling analysts about business results or by influence the business ecosystem. (Operational interactions with customers, suppliers etc. do not belong here.) As to legal and risk strategies, external audit and reporting is the core outflow of information.

3 UGF Component Descriptions

In this section, we give a description of every component of UGF.

3.1 Details of the Strategy Components

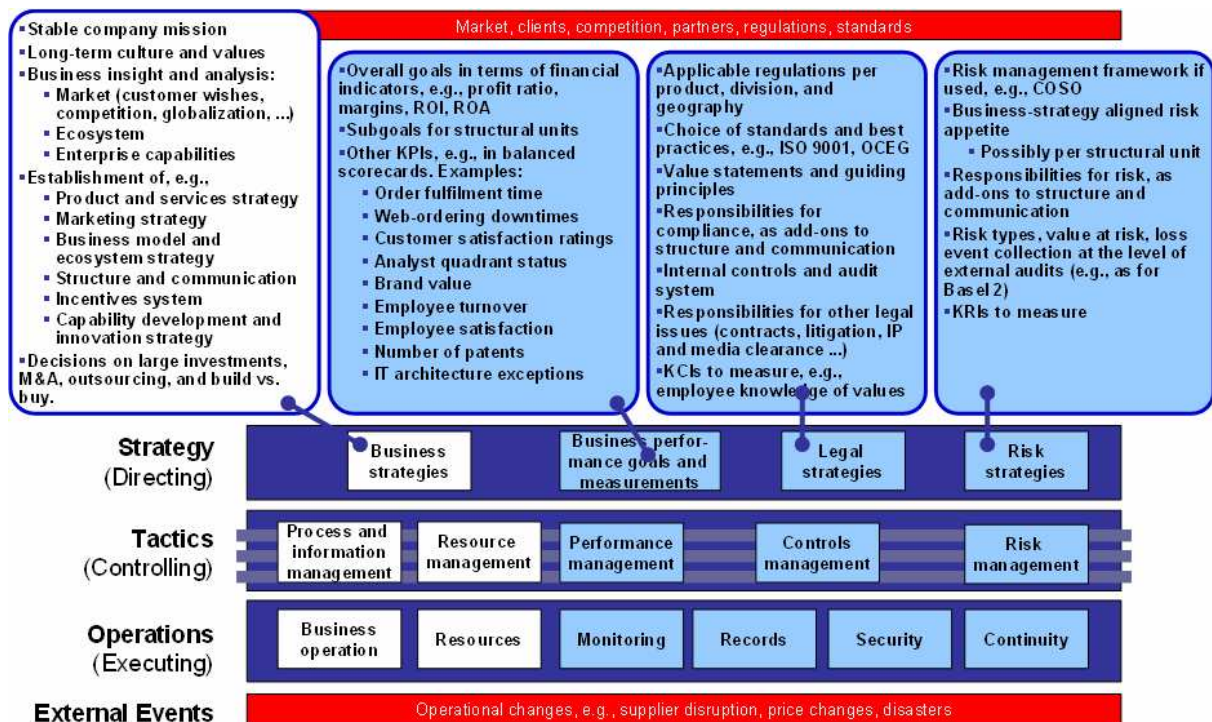The capabilities of the individual strategy components are summarized in Figure 7.

Figure 7   *Capabilities of the strategy components*

Business strategies. The business strategy component contains the standard elements of business strategies. It is important, in particular for people with an IT background, to have some knowledge of business strategies, because governance is largely strategy-driven, and the governance-specific strategies have to fit together with the overall business strategies. We can only briefly summarize business strategies here; see books such as [Gran_05].

The first important elements are a stable company mission and the long-term culture and values of the enterprise; they are informal but cannot be changed very often.

Next we list insight and analysis aspects: Clearly one needs to analyze the environment (the upper red layer), in particular the market with its customer wishes, competition, globalization etc., and the ecosystem with the suppliers, strategic partners etc. However, one also has to analyze the enterprise's own capabilities, because not all strengths and weaknesses are pre-planned.

Based on the analysis, typical strategy parts are established: The product and services strategy is what one wants to sell. The marketing strategy is how one wants to sell it. The business model decides how one hopes to make money by it. The other three capabilities listed in Figure 7 concern the internal organization: the enterprise structure (lines of business, functional units etc.) and communication model, the incentives system, which aims at aligning goals of individuals and business units with strategic goals, and longer-term goals about innovation and workforce development.

The business strategies also contains the normal IT strategy, such as developed by or with a CIO. From a business perspective, IT is a resource like human resources and facilities, and falls into strategy areas such as structure and innovation.

Business performance goals and measurements. This component handles quantitative business goals. The primary goals for a business are financial. The first choice is for which financial indicators the enterprise optimizes (such as growth versus margins); the second choice is the actual numeric goals. The overall goals are then broken down according to the product and services lines and the enterprise structure, as far as those are determined in the business strategies component.

Furthermore, many key performance indicators (KPIs) are defined. These are measurable values, but their contribution to the financial results is typically only known by statistic correlation. KPIs are used because no sure way is known to achieve financial results, or for forecasting whether the financial results will be achieved. The KPIs mentioned in Figure 7 exemplify the wide range of possibilities: Order fulfillment time and web-ordering downtime are concrete, IT-related goals; some such goals are really set on the strategy layer. Customer satisfaction ratings and analyst quadrant status are obtained by interviews, directly or indirectly. Brand value is an indicator with a real economic definition. Employee satisfaction and turnover indicate the health of internal structures and incentive systems. The number of patents may demonstrate innovation. The architecture exception number, which should be neither too small nor too large, shows how well (IT) architectures work.

The later review of the measured KPIs and the analysis of achieved financial results also belongs to this component; recall the information upflows in Figure 6.

Legal strategies. This is arguably the most important component in a modern governance architecture. At least it is the most distinctive component, corresponding to the strong driving role that compliance plays governance. Hence regulatory considerations lead the list of capabilities in Figure 6. While the regulations come from the environment, the enterprise has to determine which ones are applicable to its products and services and in the geographies of addressed markets and

enterprise facilities. Next, the enterprise may choose additional standards and best practices to follow, either as widely recognized refinements of regulations, or because the market (e.g., investors and rating agencies) demands it, or because it seems useful for financial performance (e.g., quality standards). Value statements and guiding principles are an important strategy factor chosen internally, e.g., see IBM's values at http://www.ibm.com/ibm/values/us/.

After the regulations, standards, etc. have been chosen, responsibilities and internal structures for implementing them have to be established. An example is to assign a Chief Compliance Officer, to give him or her a team, and to extend certain RACI diagrams by these new roles. Responsibilities for other legal issues must also be assigned, e.g., for contracts, litigation, and clearing information for external communication.

Finally, one may define key compliance indicators (KCIs). This is not yet a usual action nor a usual term, but corresponds to the KPIs under "business performance goals and measurements" and the later KRIs (key risk indicators). An example can be a survey how well the employees know the enterprise values, or how much they trust a whistleblower program.

The later review of the KCIs and the actually achieved compliance (e.g., numbers of known violations) also belong to this component.

Risk strategies. The third strategic component for governance is risk strategies. The importance of risk strategies has also only recently been recognized, in particular outside the insurance and financial sectors, which do core business with risk. Even in those sectors explicit management of operational risk has only recently started, in particular because of the Basel 2 requirements (the Basel Committee on Banking Supervision's "New Basel Capital Accord"). For larger parts of the industry, the US Sarbanes-Oxley Act requires a risk management framework, and such frameworks are now introduced even by other enterprises, because enterprises and investors increasingly believe that risk management is useful.

In the risk strategies component, the first choice is about using a standardized risk management framework; the following decisions are then within this framework. An important decision is about the risk appetite of the enterprise, in particular for specific structural units. For instance, one may allow certain high-risk innovative products, but impose strict risk limitations in other business units.

Next, responsibilities for risk management are assigned and aligned with other enterprise responsibilities. One may also decide on a risk classification already on the strategy level, in particular as far as losses have to be reported externally according to regulations or standards. Finally, there will be strategy-level key risk indicators (KRIs). Like KPIs, their relation to actual risk may only be known by statistic correlation or even only guessed at present, not always by clear cause-and-effect chains.

The later review of the KRIs and actual losses, at the level of detail as the risk strategy is defined, also belongs to this component.

3.2 Details of the Tactics Components

To a large extent, the tactics components work out the details of how the enterprise intends to achieve its strategic goals. The capabilities of each component are summarized in Figure 8. Again we first describe the (white) components that summarize normal tactics capabilities, because the governance-specific activities have to be at the same degree of detail and in the same terms.
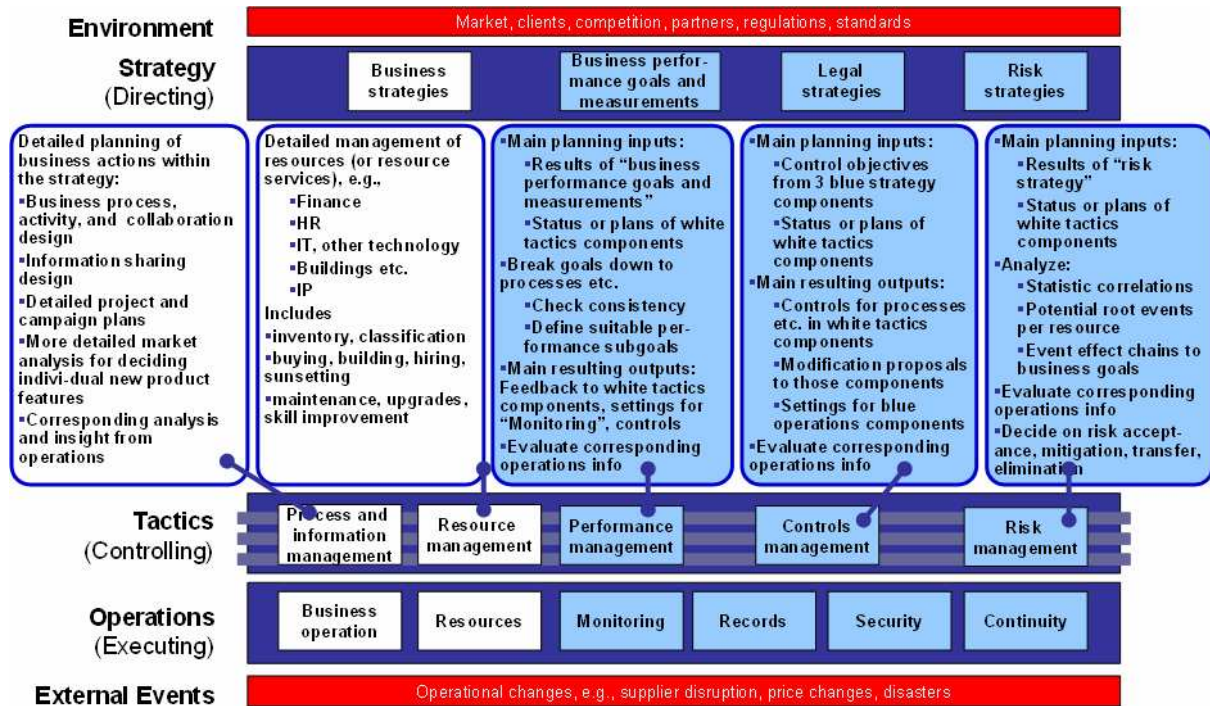
Environment — Market, clients, competition, partners, regulations, standards

Strategy (Directing)
- Business strategies
- Business performance goals and measurements
- Legal strategies
- Risk strategies

Detailed planning of business actions within the strategy:
- Business process, activity, and collaboration design
- Information sharing design
- Detailed project and campaign plans
- More detailed market analysis for deciding individual new product features
- Corresponding analysis and insight from operations

Detailed management of resources (or resource services), e.g.,
- Finance
- HR
- IT, other technology
- Buildings etc.
- IP
Includes
- inventory, classification
- buying, building, hiring, sunsetting
- maintenance, upgrades, skill improvement

- Main planning inputs:
  - Results of "business performance goals and measurements"
  - Status or plans of white tactics components
- Break goals down to processes etc.
  - Check consistency
  - Define suitable performance subgoals
- Main resulting outputs: Feedback to white tactics components, settings for "Monitoring", controls
- Evaluate corresponding operations info

- Main planning inputs:
  - Control objectives from 3 blue strategy components
  - Status or plans of white tactics components
- Main resulting outputs:
  - Controls for processes etc. in white tactics components
  - Modification proposals to those components
  - Settings for blue operations components
- Evaluate corresponding operations info

- Main planning inputs:
  - Results of "risk strategy"
  - Status or plans of white tactics components
- Analyze:
  - Statistic correlations
  - Potential root events per resource
  - Event effect chains to business goals
- Evaluate corresponding operations info
- Decide on risk acceptance, mitigation, transfer, elimination

Tactics (Controlling)
- Process and information management
- Resource management
- Performance management
- Controls management
- Risk management

Operations (Executing)
- Business operation
- Resources
- Monitoring
- Records
- Security
- Continuity

External Events — Operational changes, e.g., supplier disruption, price changes, disasters

Figure 8   *Capabilities of the tactics components (model, develop, deploy)*

Process and information management. This component contains the detailed planning of business actions within the structures and towards the goals given by the strategies. One key activity is to design detailed business processes, activities, and collaborations. Another is to plan what business information is collected and shared and how; this is often supported by IT. Detailed product and services features and how to realize them are also decided here. For one-time activities, project and campaign plans are developed. All this planning has to be accompanied by feedback and insights from the operation layer.

Resource management. This component contains the detailed planning of resource management outside specific business processes. Typical resources handled in this way by separate functional business units are finance, HR, IT, other technology depending on the sector of the enterprise, buildings, and sometimes IP (intellectual property). One class of activities to plan is resource classification and inventorying. For IT this means setting up a configuration management data base (CMDB); for HR it means high-level identity management and a skills database. Another class of activities is to provide new resources by purchase or in-house development, the integration of these resources, and later sunsetting. For IT this is buying or design, development, deployment, and later deprovisioning; for HR it is hiring, training, placement, and offboarding. Also existing resources need further development, e.g., upgrades in IT and training in HR.

Performance management. This component breaks the performance goals from the strategy layer down to the level of detail of the process and information management component. In particular, it is responsible for planning resource allocations, timelines, and priorities. This may involve proposals to redesign a process or a project. Furthermore, detailed measurements are defined here for tracing the performance on the operations layer. These measurements correspond to the performance collection information arrow in Figure 5 and mostly go into the monitoring infrastructure.

Controls management. This component establishes detailed controls to be executed in the business processes, information handling, and resource management. In particular, the controls have to be suitable to achieve the goals from the legal strategies, corresponding to the arrow "control objectives" in Figure 5. However, some control objectives also come from performance goals and risk strategies. Internal controls is typically a well-established unit in an enterprise, but the new regulations discussed in the introduction have added requirements, in particular on documentation and on the depth of controls for preventing insider fraud and identity theft. This has brought IT firmly into the picture, both as an important governance-enabling technology, and as a resource that needs more controls, in particular in change management, access management, and continuity. Correspondingly, there are many new controls, some as explicit steps in business and IT processes, others as settings for the governance components on the operations layer.

Like all tactics components, controls management also comprises evaluating the results, in particular control tests and detailed audits.

Risk management. Even if great plans are made in the preceding tactics components, there is almost no sure way to achieve any strategic goals (and if there is any, it is costly). This is where risk management comes in. It evaluates factors that may lead to goals being missed, evaluates their likelihood, and makes action plans for dealing with these factors. Actions can mean to simply accept a risk (if the risk appetite from the strategy layer is sufficient), to reduce the risk by additional measures in the concerned processes or resources, to transfer the to others, e.g., by insurance, or to eliminate the risk, e.g., by not building a certain product. A major novelty in recent years is that operational risk is considered in detail; this is everything besides market and credit risks, from leaking roofs over IT failures to internal or external fraud.

Two approaches at risk analysis and forecasting will continue to coexist for a long time: purely statistical approaches and attempts to find complete cause-and-effect chains. The statistical approach evaluates the types and sizes of prior losses and tries to correlate them to certain influenceable factors, which are either known KRIs or may become KRIs. The action plans are then based on the identified important factors. The other approach attempts to find root causes of negative events, and to follow all effects that they can have in the enterprise. Doing this comprehensively requires very detailed business process and resource models from the components "process and information management" and "resource management". For most types of operational risk, both approaches need better data collections than currently available.

3.3 Details of the Operations Components

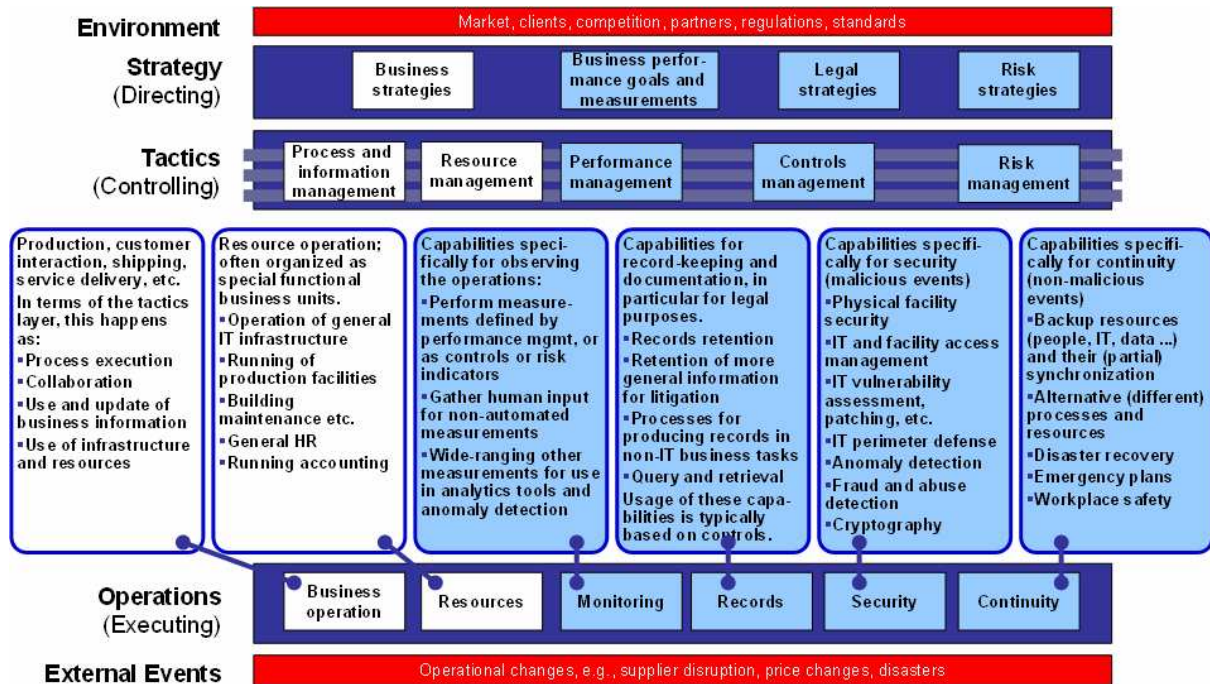The capabilities of the individual operations components are summarized in Figure 9.

Figure 9   *Capabilities of the operations components*

Business operation. This is the normal running of the business, e.g., production, customer interaction, product shipping, and service delivery. It follows the business processes, activities, collaboration patterns, and project plans from "process and information management", and populates and uses the information infrastructures planned there. The execution comprises people as well as IT, e.g., specific business applications, process or workflow execution engines, and information systems.

Resources. This is the normal operation of resources, as planned in "resource management". For instance, for HR this includes the day-to-day actual hiring of people, for facilities it includes cleaning and repairs, and for IT it includes user interactions and event handling.

Monitoring. The monitoring component contains capabilities for observing the operations. Monitoring is seeing a strong growth of IT as a governance-enabling technology. However, recalling our examples of KPIs, KCIs, and KRIs, one should not forget that explicit human inputs are still very important for some business-level data collections. Important input for what needs to be monitored is the performance collection information from "performance management", but the controls and risk management also have monitoring needs. The monitoring infrastructure also contains analytics components, in particular for the statistics-based detection of anomalies, which it then passes to more specific components for evaluation. We present the monitoring infrastructure in more detail in Section 4.

Records. The records components answers a multitude of new requirements for well-organized document retention. This includes capturing all information that needs to be retained for certain periods of time by regulations or that might be needed in litigation (e.g., email capture), ensuring that the information is really not deleted (i.e., retention policies across all storage layers), integrity of the retained information, and long-term archiving. A high-end capability is provenance, i.e., storing information with enough metadata that graphs of the origin of the information can be

reconstructed when needed; this is increasingly important for accountability. The detailed policies or settings for the records component typically come from the controls management.

While the new IT aspects currently dominate the discussions, the integration with the handling of paper documents and the recording of physical actions is also very important.

Security. A comprehensive and well-managed security infrastructure has become a must for several new regulations. It is also very useful for enforcing other governance aspects and for risk reduction. The focus is on increased IT security, but also HR and facilities are concerned, e.g., with increasing background checks for employees and increased physical security. Roughly, the role of security in governance is to enforce that people remain within their prescribed decision rights. Furthermore, one attempts detect and analyze whether peoples' behavior within their decision rights is unusual and a potential problem. Important IT security capabilities are access management and the underlying identity management, IT vulnerability detection, prevention, and patching, and perimeter defense. Data encryption has also seen a strong rise in real life, in particular because a series of laws starting with the California Senate Bill 1386 requires that an enterprise notifies its customers when it leaks personal information usable for identity fraud.

Continuity. The continuity component defends against adverse events that occur without malice, while security defends against intelligent, malicious fraud attempts. A core measure is to provide backups for important resources such as people, IT components, and data, together with processes to keep the backup resources sufficiently synchronized with the primary resources so that they can take up the work if needed. Standard backups are as similar as possible to the primary resources, but it is also useful to have some backup processes and different resources in case there is a systematic error in the primary process or resource type. One also needs emergency and disaster recovery plans, detailing how one fights the disaster, giving overall plans for organizational structures during or after a disaster, and providing training. Workplace and facility safety measures also belong to this component. Detailed choices about how much continuity infrastructure is used typically come from the risk management component.

4 Drill-Down Example: Monitoring Infrastructure

In this section, we use the monitoring component as an example of how one can drill down into a UGF component. We only consider IT-based monitoring now. The level of detail is such that one can start identifying actual service interfaces and options for technical synergies. Figure 10 corresponds to the lower left corner of Figure 4, with the monitoring component on the right and the components "business operation" and "resources" on the left; we only arranged them vertically now for a nicer layout.

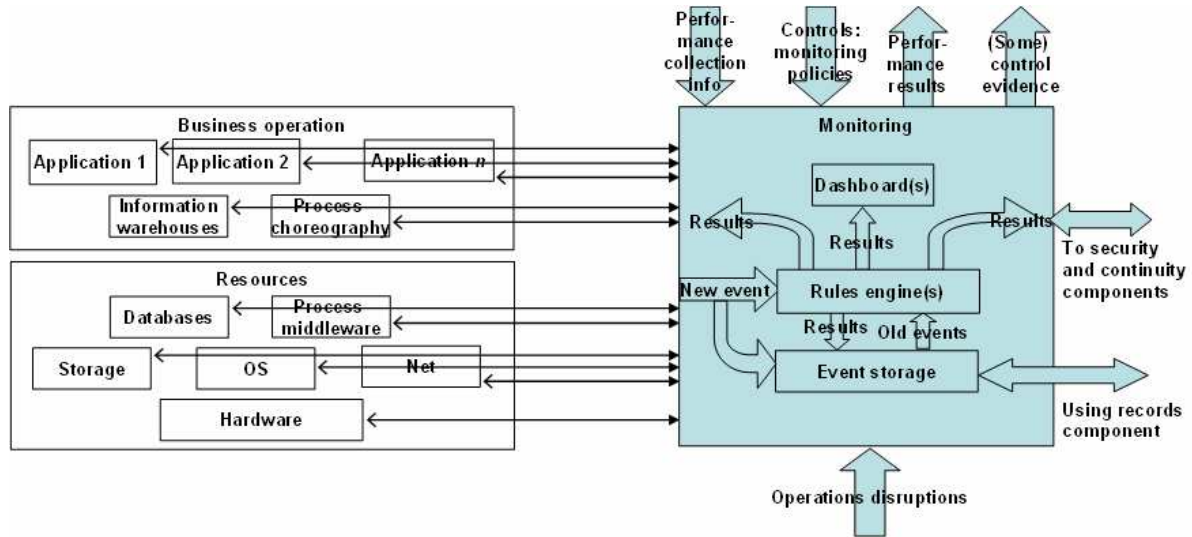# 4.1 Subcomponents and Information Flow

Figure 10   *Drill-down into the monitoring infrastructure*

The monitoring component may receive events from all the other components, here exemplified with typical subcomponents of the business operation and resources components. The normal components need adapters for this. Logically the adapters also belong to the monitoring infrastructure, in particular if they are configurable. Technically, the adapters are typically event interfaces or extensions of log interfaces; for networks they may also be separate sniffers or gateways. The events monitored at a component include the component's "own" events and events belonging to higher components. For instance, on the arrow from the subcomponent "Net", there are network management events as well as sent and received messages that logically belong, e.g., to certain applications. Finally, there may be directly sensed events from the external environment on the arrow "operations disruptions", e.g., coming in via smoke sensors.

In the core monitoring infrastructure, the events are handled by rules engines, from very efficient simple filters to complex analytics engines. In addition, either all events may be stored or only those fulfilling certain rules. The event storage may use the records component, in particular if retention requirements exist for certain events. Stored events may be reused by rules engines.

Results of a rules engine can be shown on a dashboard in the monitoring component; most rules engines offer at least a simple dashboard. However, monitoring results are also used by many other components. In particular, they are the main contributions to the upward arrow "performance results"; the rules (policies, settings) for what results are reported come from the downward arrow "performance collection information". Monitoring results also contribute to the arrow "control evidence", based on controls that have been implemented as monitoring. Furthermore, the security and continuity components rely on monitoring; hence there are also rules that recognize security and continuity events. Finally, there may be feedback from monitoring to subcomponents of the components business operation and resources, although this is less usual at present.

4.2 Benefits

The benefit of investigating monitoring as such a technology-neutral structure is that one can use this structure to classify individual products and components and to achieve synergies. One opportunity for synergies is that several rules engines share the same event adapters on the various applications, middleware components, etc. Common event stores are another opportunity. Furthermore, one can study whether analyzing for different types of outputs, e.g., performance results, security events, and continuity events, needs separate rules engines or only different rules in the same engine.

Correspondingly, one can classify products or existing monitoring solutions by questions like the following: Which sub-components do they focus on and how? What assumptions do they make about the event representation and the available event storage? Do they come with their own dashboard, and/or how can they the forward results to other components?

5 Scenario 1: Business Controls Automation

Our first scenario shows how UGF can be used to analyze a business-level scenario, and how interoperable capabilities in all UGF components can simplify the implementation of such a scenario. We consider a use case that currently occurs in many enterprises: the automation of Sarbanes-Oxley (SOX) controls. The Sarbanes-Oxley Act is a regulation and mandatory for public companies listed in the US. As it has been in effect for a couple of years already, one might think that no further efforts are needed for it, but this is not the case; in fact, in particular software spending for it is still on the rise.
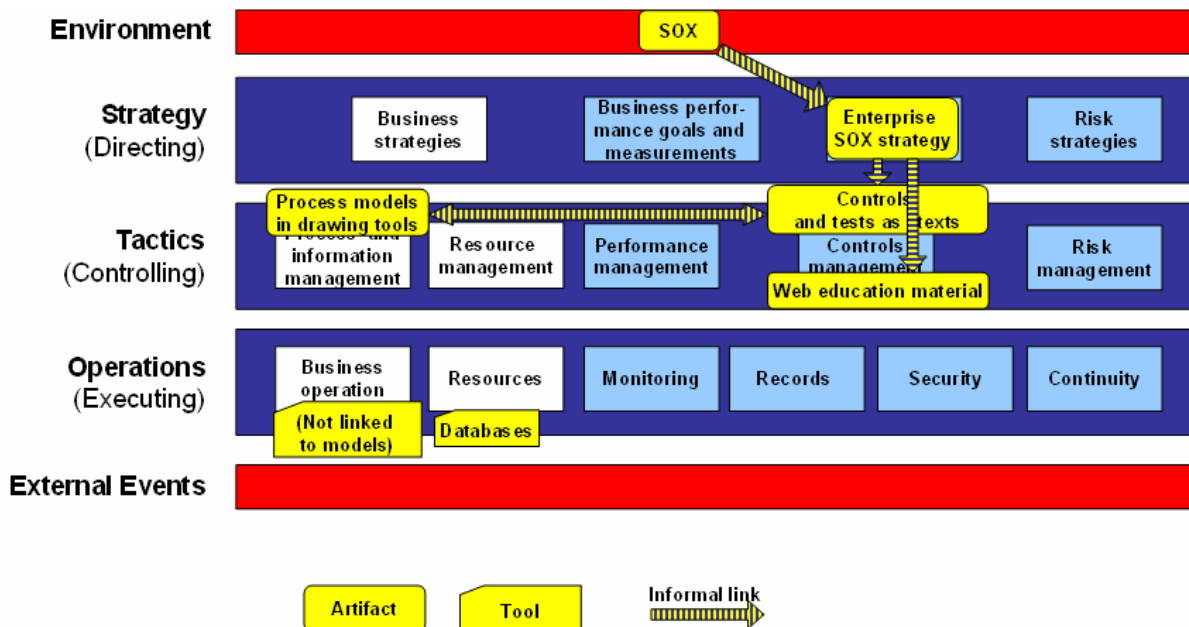

Figure 11   *A typical current situation for business controls*

A typical current situation is shown in Figure 11. A company that needs to comply with SOX will have an enterprise SOX strategy already. On the tactics layer, it must have a detailed set of controls and tests for them. Typically the controls and tests are only described as texts. There may or may

not be an IT-based management system for keeping track of them and the test execution. The controls have to be linked to documentations of the business processes that handle financial data; usually these processes are depicted as workflows in drawing tools. There may also be education material for the controls; note that controls are typically executed by normal operational personnel, e.g., a travel request may be approved by the manager of the employee who wants to travel.

However, there is typically no link yet to the operations layer: The business process execution is neither directly linked to the drawings nor to the controls education material. Hence also that documentation arising in the process execution, shown as databases in Figure 11, is not directly linked to the controls. This is one reason why control testing is currently a huge manual overhead: Relevant material must be requested, retrieved, and evaluated.

It is also easily possible that a control test fails. For instance, the process drawings are not always sufficiently detailed to make clear what documentation must be stored. Furthermore, due to the textual description of the controls and the test, the descriptions may differ slightly, or the people reading them may interpret them differently. Failed tests cause additional work and may ultimately delay financial statements, which is very bad for the reputation of an enterprise.

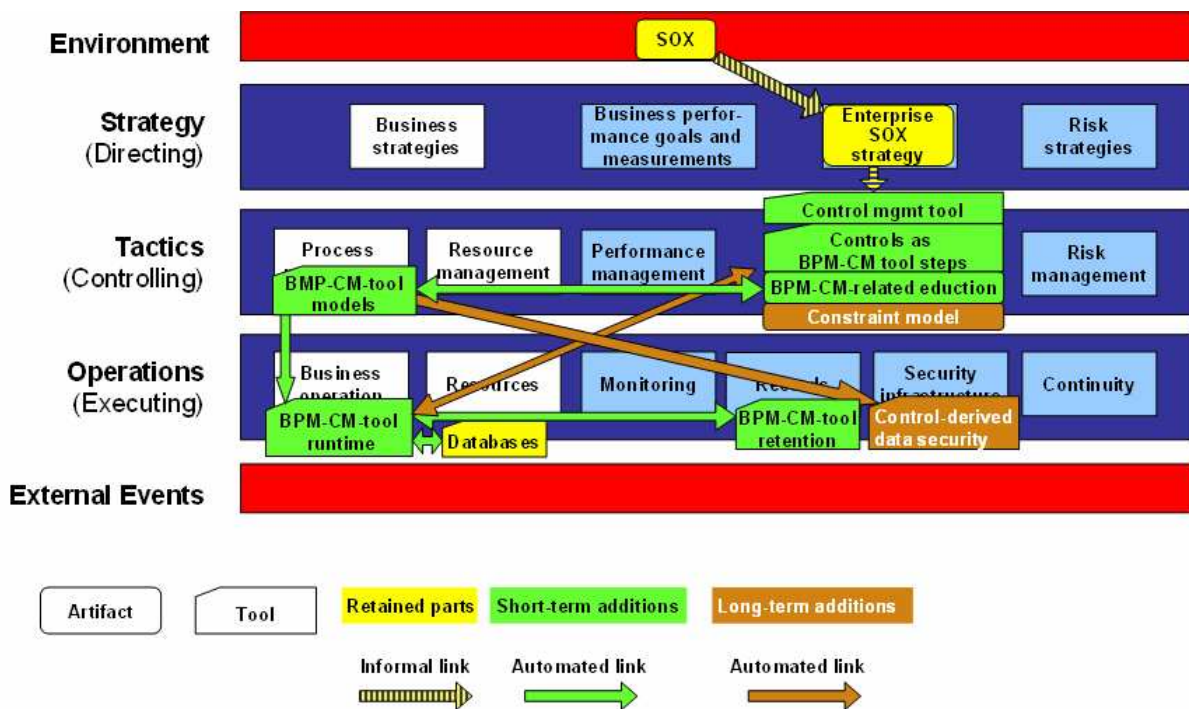Figure 12 shows a desirable, more automated version.

Figure 12   *Example of a more automated version of the situation in Figure 11*

The main addition is to use a runtime business process and content management tool for the process under consideration, we abbreviate this by BPM-CM-tool; among IBM products we are thinking of FileNet. The first change is that the business process is modeled not in a drawing tool, but in the modeling part of the BPM-CM-tool. This enables an automated and consistent link to the operation layer, here called "BPM-CM-tool runtime". Furthermore, the BPM-CM-tool enables detailed modeling of the data involved in the process, and again this will be consistently handled in the

runtime. One can even link existing data repositories in, i.e., one only needs to reorganize the information architecture if one wants to use new features such as better retention policies.

Furthermore, we have added a dedicated control management tool, such as WBCR (IBM Workplace for Business Controls and Reporting) in IBM's product suite.

If we now describe a control that needs automation in the controls management tool as a detailed FileNet steps, we solve several of the issues mentioned above at once: The step description makes it clear on what documents the control is to be based. Hence we can ensure once and for all that these documents will be stored at runtime. Appropriate retention policies ensure that the documents survive long enough. We can even describe the test in FileNet terms now and thus ensure that the test is only based on well-defined and stored documents. As far as the control is automatable, we can also actually automate it. Many controls are partly automatable and partly need human judgment. As a simple example, a control on a travel request by a software engineer may require that only economy class flights are used, that the trip takes no longer than 3 days, and that it goes to the location of an existing customer of the business units or to a learning event recognized by the enterprise. However, there will be human judgment whether the trip, even if within these bounds, is really necessary, and often there will be an exception process for approving some travel requests outside the standard bounds. For the human control action, a description can be integrated with the BPM-CM-tool.

Longer-term, two further automation steps are conceivable: A general constraint language for controls against which the concrete implementation can be validated, and setting data security policies automatically from the control properties.

6 Scenario 2: Strategic Access Control

As a rather different scenario from that in Section 5 we consider access control. Security and thus access control are typically thought of as IT governance, and indeed security is a UGF component on the operations layer. However, by using UGF with its emphasis on strategic goals as drivers of tactics and operations, we obtained new insights on how to set up access control in business-related ways. The overall scenario, which we call strategic access control, is shown in Figure 13.
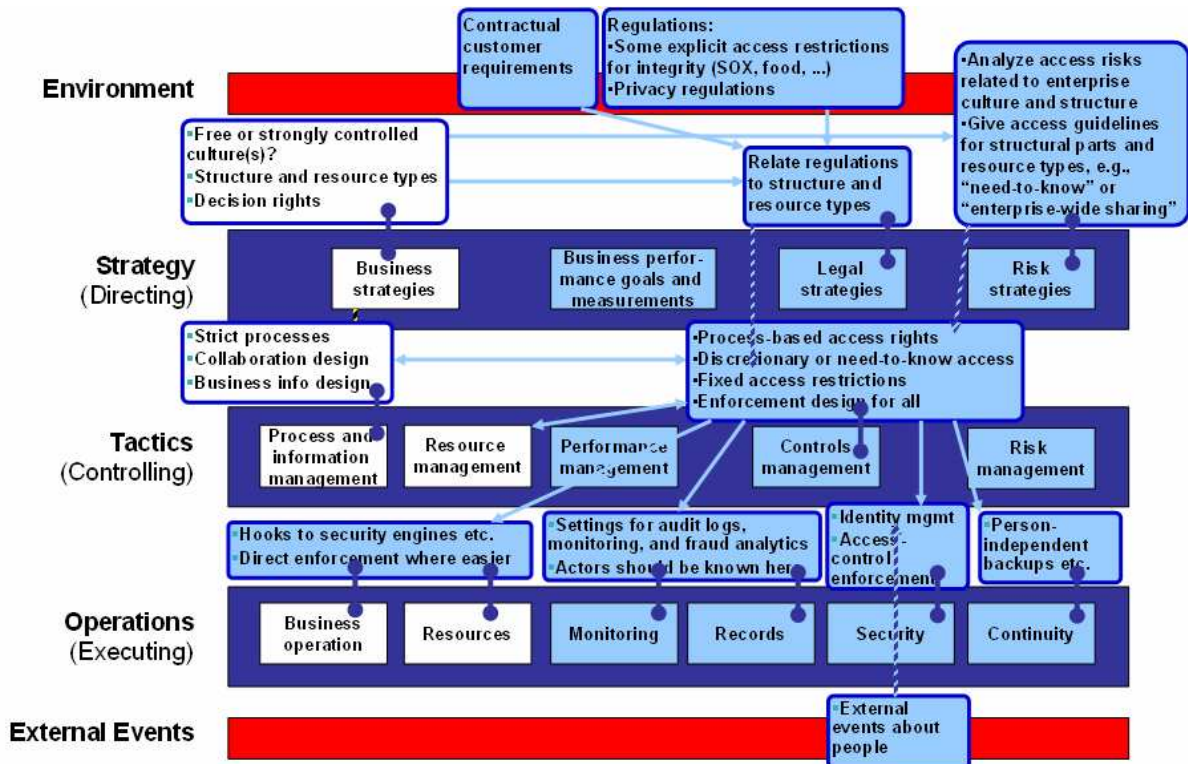
Figure 13   *Aspects of strategic access control*

6.2 Environment

Some requirements related to access control come from the environment. First, some regulations make rather explicit access restrictions. In particular, regulations such as the Sarbanes-Oxley Act and food and drugs regulations require the integrity of certain data, while privacy regulations restrict who can see certain types of data. Secondly, large enterprise customers or ecosystem partners often require confidentiality for certain data.

6.3 Strategy Layer

On the strategy layer, the main activities related to access control are in the component "legal strategies". First, one analyzes what regulations apply for which enterprise units, resource types, and geographies, and which of these regulations have access-related consequences. This analysis is based on the definition of the enterprise units, resources, and geographies in the business strategy component. Secondly, one should analyze the business strategy whether certain types of culture are prescribed for certain enterprise units, such as a large degree of individual freedom in a unit that aims at product leadership, versus strict processes for cost control in a unit aiming at operational excellence. This should lead to similarly free versus strictly restricted access rights in the respective units. Thirdly, one should specifically study the decision rights defined in the business strategies component, because they imply rights to obtain certain information and to perform certain actions.

In addition, the risk strategies component is needed to give guidance on how access should be handled between the two extremes of allowing everything that is not forbidden by law or contract, and allowing nothing unless it is needed for explicitly predefined decision rights. For this, one has

to balance the risks associated with broad access rights with the opportunities that broad access rights offer and the hassle and bad feelings that narrow access rights may cause.

While some parts of the regulations may lead to concrete access control policies already, as exemplified with privacy laws [PoAW_04], most access-related results from the strategy layer will be in other terms, e.g., they will only prescribe that "need to know" is followed for certain enterprise units or resources, leaving it to the tactics layer to specify who needs to know what. Other such results may be to only require "separation of duties" or a 4-eye principle for certain broad classes of actions or activities.

6.4 Tactics Layer

On the tactics layer, the component "controls management" is primarily responsible for access-related decisions. Its upper access-related inputs are the strategic goals we discussed in Section 6.3. These goals now have to be refined to the level of detail about the enterprise that the components "process and information management" and "resource management" provide. There are three main cases.

- For relatively concrete requirements in the form of normal access-control policies on high-level classes of actors and information, such as shown in [PoAW_04], the task is to refine the high-level classes into more concrete groups of people and types of information known on the tactics layer. For instance, groups and roles of people may be found in the HR design, and information types in the data architecture. Similarly, for separation-of-duty requirements the concerned action types from the strategy layer need refinement.

- For business units or activities where strict need-to-know is required, there is typically also a strict process-oriented design of the corresponding business unit. In this case, the access rights must be derived from the processes. In addition, one should analyze whether the process follows the data minimization principle, i.e., that people only get inputs they really need in the steps they execute. If this is not the case, redesign may be requested from the process and information management component. A typical example is not to give someone access to an entire customer record if they only need a few fields.

- For business units or activities where the legal and risk strategies allow rather free access, there is typically a collaboration design in the process and information management component. Then either access rights may be completely free in the enterprise, e.g., if the collaboration is organized in a wiki in the Intranet. Or one may delegate the actual access control to the leaders of the collaboration, e.g., by allowing them to set access control lists for an entire teamroom. Or one may delegate access control to every collaborator by allowing document owners to set access rights on their documents.

After thus deciding on more concrete access policies, the controls management has to plan the enforcement. Where strict processes are given, this enforcement will often be integrated in the process. Where certain types of data are controlled by regulations, one will put some access control enforcement close to the data repositories even if there are additional restrictions in the processes or applications, in particular to enable audits of the data accesses and modifications. Setting policies for central access-control engines in the security component on the operations layer is particularly useful if one has high-layer policies which the access monitors for individual resource types (such as files, web resources, and documents in content management) can map to actual resource descriptions.

The controls management should also ensure that access restrictions cannot be circumvented on lower IT layers, e.g., that documents protected at the content management level cannot be read by additional people at the operating systems level, and that files protected at the operating systems level cannot be read by stealing easily accessible tapes [Pfit_07]. Sometimes this may lead to select encryption instead of access control as the appropriate enforcement.

6.5 Operations Layer

On the operations layer, the measures selected on the tactics layer have to happen.

In the IT products supporting business operations and resource handling, we need call-outs to central access-control engines before every relevant access decision, or direct enforcement of the policies (e.g., in processes or by SQL query modification) where that seemed simpler, more precise, or more efficient.

The security component is responsible for the access-control policies as well as the underlying low-level identity management, e.g., for linking HR identities and roles to user names in different software tools. Extended identity management may take in external events about people, e.g., knowledge that they have relations to other people in situations where separation of duty is required.

In addition, one may make access-related settings in the monitoring and records components, e.g., to store controlled accesses for later audit and to monitor for unusual access patterns. Furthermore, the continuity component may be used to ensure availability of access even if certain people are unavailable.

Summary

We have given an overview of IBM's Unified Governance Framework (UGF). This is a framework for enterprise governance, in contrast to narrower scopes such as corporate governance or IT governance. The highest layers consist of a component model and a lifecycle. The component model is organized in a strategy layer, a tactics layer, and an operations layer. The components are chosen such that governance-specific activities are treated in more detail than normal activities. For seeing all enterprise activities at a similar degree of detail, one should use IBM's Component Business Model (CBM) instead. We showed how UGF can be used by two types of examples: One was the technical drill-down into one component, the monitoring infrastructure. This showed how needs for interoperability, internal standards as well as opportunities for cost-saving synergies can be derived from the component view. The other type of example were two scenarios. One scenario was business control automation, the other was strategic access control. They show how a comprehensive framework can help implementing both business-related and IT-related governance solutions, and how a scenario that is primarily regarded as a rather complex IT issue can largely benefit from strategic considerations.

Acknowledgments

References

AKM+_07 Carl Abrams, Jürg von Känel, Samuel Müller, Birgit Pfitzmann, Susanne Ruschka-Taylor: Optimized Enterprise Risk Management; IBM Systems Journal 46/2 (2007) 219-234.

CBM_07   IBM Global Services: Component Business Modeling; http://www-935.ibm.com/services/us/gbs/bus/html/bcs_componentmodeling.html, 2007.

Gran_05 Robert M Grant: Contemporary Strategy Analysis; Blackwell Publishing 2005.

ITGI_03 Information Technology Governance Institute: Board Briefing on IT Governance, 2nd Ed., 2003.

OECD_04 Organisation For Economic Co-Operation And Development: Principles of Corporate Governance, Revision 2004.

Pfit_07 Birgit Pfitzmann: Multi-layer Audit of Access Rights; accepted for 4th VLDB Workshop on Secure Data Management (SDM'07), Vienna, Sept. 2007, proc. to appear in LNCS, Springer-Verlag.

PoAW_04 Calvin Powers, Steve Adler, Bruce Wishart: EPAL Translation of the The Freedom of Information and Protection of Privacy Act; V1.1, IBM and Information and Privacy Commissioner/Ontario, March 2004, http://www.ipc.on.ca/images/Resources/up-EPAL_FI1.pdf.

WeRo_04 Peter Weill, Jeanne W. Ross: IT Governance: How Top Performers Manage IT Decision Rights for Superior Results; Harvard Business School Press, 2004.