## 5.3 Management Model

**Management**

> Management is the consistent monitoring, control, and reporting of the state of resources in accordance with the policies, agreements, and principles established by the associated stakeholders and between those stakeholders.

Management of complex systems embodies the concept of providing consistent and predictable system behavior under all operating conditions, normal or otherwise. Consistency is the expectation that all stakeholders within categories defined by access rights and capabilities see the same or equivalent system responses to the same system conditions. Predictability is related to consistency but has a temporal aspect in the expectation that the same response received for a condition today will be the same response to the same condition in the future, barring promulgated changes to those responses.

Traditional system management focuses on fault, configuration, account, performance, and security management functions. These functional areas are known as "FCAPS" functions based on the recommendations in ITU-T Rec. M.3400 (02/2000), "TMN Management Functions." The primary role of the functional groups is to concentrate on maintaining systems in a trusted, active, and accessible state. Systems operating in a SOA ecosystem are individually subject to these concerns, but the association with the ecosystem imposes additional complexity to the management of those participating systems, particularly where ownership boundaries must be crossed.

Individual systems are not necessarily operated or used in an environment requiring trust before the stakeholders make use of the system. Indeed, many of these systems exist in hierarchical management structures within which use may be mandated by legal requirement, executive decision, or good business practice in furthering the business' strategy. Successful operation of a SOA ecosystem requires trust between the stakeholders and the component systems. This trust may be established by agreement, policy, or implicitly through observation or repeated interaction with other systems. The implicit trust component adds fragility to the management of a SOA ecosystem since failure to facilitate consistent, predictable interactions undermines the trust between participants and within the ecosystem as a whole.

Management in a SOA ecosystem is thus concerned with managing the resources in the ecosystem so that consistent and predictable ecosystem behavior is maintained while also maintaining consistent and predictable trust relationships. These concerns should largely be handled within the governance of the ecosystem. The policies, agreements, and practices defined through governance provide the boundaries within which management operates and for which management must provide enforcement and feedback. However, governance cannot anticipate all

circumstances and must provide sufficient guidance in areas where anticipation is unclear or for which agreement between all stakeholders cannot be reached. Management in these cases must be flexible and adaptable to handle unanticipated conditions without unnecessarily breaking trust relationships.

In the SOA ecosystem, the traditional managed system resources are present but expanded to include new classes of resources. These new resources consist of the policies and agreements agreed to by the stakeholders through the governance processes, participant interactions, participant relationships, and resources unique to SOA ecosystems related to the use of services across multiple ownership domains. Management control must be capable of acting across all ownership domains and in a consistent fashion. Additionally, the results of monitoring and reporting must be made accessible to all participants in all ownership domains. This suggests that the management functions and information are provided as services within the ecosystem and consumed in the same way as other services. Thus, management functions and information become a resource that must be managed.

The ability of participants to provide services to users from other ownership domains or to consume services offered in other ownership domains raises issues not found in traditional system management. These issues are particularly profound in ecosystems that are highly decentralized in which the participants interact as peers, possibly through mediation services, and for which no centralized operational authority exists. Notwithstanding questions of who is responsible for ensuring that infrastructure capabilities are managed, there exist issues associated with ownership rights, financial responsibility, ecosystem fault or failure responsibility, and enforcement responsibility.

The management model described here is intended to convey how the SOA framework applies to managing, using, and providing services. A representation of the management model is shown in Figure xxx. Management services differ from other services through the requirements to manage those characteristics of services that can be considered as service metadata such as service lifecycles, attributes associated with service use, and the relationships between services.

The concept of service metadata described in the previous paragraph is more precisely defined as an attribute or property of a service that is manageable, i.e., capable of being monitored, controlled, and reported on. These manageability properties are not unique to individual services but should be identifiable for any service consumed or supplied within the ecosystem, including the management services. The necessary existence of these properties within the SOA ecosystem motivates the following definitions:

**Manageability Property**

A property of resources that can be monitored, controlled, and reported on. Such properties are generally considered to be external to the managed resource but may result from processes or structure within the resource.

Manageability properties are the fundamental unit of management in systems management. These properties may be grouped by applicability to certain categories of resources for which the property has relevance. These categories of manageability properties represent capabilities that are managed through their representation in the manageability properties.

**Managed Capability**

A collection of manageability properties representing different aspects of the same capability.

Management of these capabilities is identified by the capability name followed by the word "management." For example, the managed capability consisting of configuration manageability properties is referred to as "Configuration Management." Resources not managed under a particular capability are resources for which the manageability properties making up the capability have no clear meaning or use. As an example, all resources within a SOA ecosystem have a lifecycle that is meaningful within the ecosystem. Thus, all resources are manageable under Lifecycle Management. In contrast, all resources do not report or handle events. Thus, Event Management is only concerned with those resources for which events are meaningful. The following capabilities are managed capabilities applicable to a SOA ecosystem. They do not define an exhaustive list but represent the most common capabilities for which management must be defined.

**Lifecycle Management**

Management of the properties associated with the creation, existence, and destruction of resources. These properties may include the necessary state of the ecosystem for the creation and continued existence of the resource, the means for creating and destroying the resource, and the state of the ecosystem following the destruction of the resource.

**Configuration Management**

Management of the properties associated with resource state, the relationship of the resource to the ecosystem, or the state of the ecosystem (when considering the ecosystem as a manageable resource). Configuration management should involve management of resource versions and management of the deployment of new services into the ecosystem and the removal of old services from the ecosystem.

**Event Management**

Management of the properties associated with events, the generation of events, the handling of events, and the identification of event types.

**Security Management**

Management of the properties associated with the security of resources including identification of roles, permissions, access rights, and policy attributes defining security boundaries and events that may trigger a security response.

Security management within a SOA ecosystem is essential to maintaining the trust relationships between participants residing in different ownership domains. Security management must consider not just the internal properties related to interactions between participants but ecosystem properties that preserve the integrity of the ecosystem from external threats.

**Quality of Service Management**

Management of properties identified as indicators of the quality of service provided by resources. Examples of these properties include network latency limitations, bandwidth requirements, or roundtrip response time. Quality of Service properties may be used as consumer requirements for service providers, provider requirements for consumer use, or overall ecosystem performance requirements for participants.

**Usage Management**

Management of those properties associated with the use of resources. Usage management includes access management properties, demand management properties, and financial management properties. Access management properties include how the resource is accessed, who is using the resource, and the state of the resource after use. Related to access management is demand management concerned with properties related to controlling or shaping demand for resources to optimize the overall operation of the ecosystem. Financial management properties are those associated with assigning costs to the use of resources and distributing those cost assignments to the participants in an equitable manner.

**Policy Management**

Management of the properties associated with enforcement of policies, distribution of policies, the trigger points for the activation of polices, and the validity of policies.

Other managed capabilities exist which are important in some SOA ecosystems and not important in others.

### 5.3.1 Monitoring and Reporting

The successful application of management relies on the monitoring and reporting aspects of management to enable the control aspect. Monitoring in the context of management consists of reading data from a manageability property and evaluating that reading in relationship to some expectation. Monitoring in a SOA ecosystem is enabled through the use of mechanisms by resources for exposing manageability properties. In the SOA framework, this mechanism may be a service for obtaining the reading. Alternatively, the reading may be monitored by means of event generation containing updated values of the property.

Approaches to monitoring may use a polling strategy in which the readings are requested from resources in periodic intervals, in a pull strategy in which the readings are requested from resources at random times, or in a push strategy in which the readings are supplied by the resource without request. The push strategy can be used in a periodic update approach or in an "update on change" approach. Management services must be capable of handling these different approaches to monitoring.

Reporting is the complement to monitoring. Where monitoring is responsible for obtaining measurements, reporting is responsible for distributing those measurements to interested stakeholders. The separation between monitoring and reporting is made to include the possibility that data obtained through monitoring might not be used until an event impacting the ecosystem occurs or the measurement requires further processing to be useful. In the SOA framework, reporting is provided as services for requesting measurement reports. These reports may consist of raw measurement data, formatted collections of data, or as the results of analysis performed on measurement data from collections of different manageability properties. Reporting is also used to support logging and auditing capabilities, where the reporting mechanisms create log or audit entries.

### 5.3.2 Management and Governance

Governance in a SOA ecosystem provides a trusted context for participant interaction and forms a basis for negotiation and agreement between participants. The results of governance are policies, guidelines, and principles used to define the boundaries of the ecosystem, the meaning of trust within the ecosystem, and what participating in the ecosystem requires through what is permissible and what is not.

The outcomes of governance provide no value to the ecosystem if there is no mechanism for ensuring that the policies are followed, the guidelines are used, and the principles are appropriately applied. This is the role of management and this role defines the relationship of management and governance. Governance is a legislative element of the SOA ecosystem and management is the corresponding executive element. Thus, management must ensure compliance to policy, use of guidelines, and adherence to principles through the various management functions discussed previously.

Similarly, effective management in the SOA ecosystem requires an ability for governance to understand the consequences of its policies, guidelines, and principles and to adjust those as needed when inconsistencies or ambiguity become evident from the operation of the management functions. This understanding and adjustment must be informed by the results of management and so mechanisms for providing feedback from management into governance must exist.

### 5.3.2 Management and Security

We previously discussed security as managed capability. In fact, there is a much closer relationship between management and security. Security in the SOA ecosystem relies on accurate and timely monitoring and reporting of measurement data from the other managed capabilities to ensure the integrity of the ecosystem. Depending on the priorities set by governance, management must ensure that the appropriate prioritization is applied to properties that might be considered critical to security management.

In addition to security management in the SOA ecosystem, there is the concept of security of management. This concept defines how management data is provided to stakeholders such that the integrity of the data is unquestionable. Since much of the interactions between stakeholders in the SOA ecosystem is based on trust, the ability to put trust into another domain or be accepted as a trusted domain depends on the ability of the infrastructure to ensure the security of critical management data. This in turn requires identification of critical management data and policies associated with the handling of that data be made by governance.

### 5.3.3 Management Infrastructure

All of the properties, policies, interactions, resources, and management in the foregoing discussion are only possible if an infrastructure providing support for management capabilities exists. Each managed capability imposes different requirements on the capabilities supplied by the infrastructure and the SOA ecosystem concept requires that those capabilities be usable as services or at the very least be interoperable.

Fundamentally, an infrastructure enabling service management must support

1. Integration with security services
2. Monitoring services
3. Reporting services
4. Health services (e.g., heartbeat, ping)
5. Alerting services
6. Lifecycle access services (and associations with health services)
7. Logging, auditing, and the integrity of these such as non-repudiation and consistent ecosystem timing
8. Service versioning management at runtime or at request time
9. Service discovery
10. Service mediation, protocol mediation, ecosystem federation

11. Messaging including routing, persistence, redirection, unicast, broadcast
12. Recovery capabilities such as failover, hot swap, redundancy in critical components
13. Basic System and Network Management capabilities such as
    a. Scalability capabilities such as load balancing, redundant service identities
    b. Quality of service monitoring and runtime management of service level agreements, contracts, and other agreements
    c. Mechanisms for ensuring that availability, response times, throughput, and latency targets are met
    d. Fault identification, isolation, correction
    e. Support for maintenance activities without impact to the overall operation of the ecosystem
    f. Deployment of infrastructure capabilities in a distributed or federated environment

Other infrastructure capabilities that aid management within large SOA ecosystems include data brokering services, transaction management services, and time services that provide consistent times across ownership boundaries spanning multiple, heterogeneous hosting platforms and geographical locations.

### 5.3.4 Management and the Service Lifecycle

The application of management to the service lifecycle requires a consistent definition of that lifecycle across the ecosystem and the infrastructure components to support control and monitoring of that lifecycle. Additionally, for management of the lifecycle to ensure consistent and predictable behavior in the ecosystem, the services must provide information that is sufficient to ensure that the service is usable in the ecosystem. This usability consists of a description of the dependencies on other resources that must be satisfied for successful creation of the service, changes in dependencies as the service progresses through different states in the lifecycle, and the actions to be expected from the service when it is destroyed.

From a management perspective, managing these dependencies requires the ability to ensure that the dependencies can be satisfied and if not, delay the creation of the service or the progression of the service to new states in the lifecycle while maintaining service levels or other contractual requirements. These dependencies may require the creation, reconfiguration, or destruction of other services or resources in other ownership domains. Understanding the effect of destroying a service requires that the management of the lifecycle ensure that state within the ecosystem is not corrupted or compromised at the destruction of a service. Governance policies should ensure that such effects are mostly prohibited but the enlistment of outside services may create destruction dependencies that were not anticipated.