Chapter 1

Introduction

Solutions in this chapter:

- **NetWeaver Web Application Server**
- **ABAP WEB AS 7.0**
- **J2EE WEB AS 7.0**
- **Backend UNIX/Oracle**
- **Governance, Risk, and Compliance (GRC)**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

When you consider the changes in SAP over the years, it's an evolution that is both amazing and inspiring. The vision of R/3 back in 1993 compared to where it is today, 15 years later, highlights its initial purpose. That purpose was to enable business to be more efficient, effective, and integrated. Those of us that studied process engineering and realized that the decentralized information technology (IT) culture and islands of automation we had in the 1980s and early 1990s were ineffective in helping business evolve, understood this need for an integrated enterprise solution.

Rudy Puryear[1] of Accenture Consulting discusses the evolution of IT systems from the 1970s to today. He describes three phases of an electronically driven economy. These phases are about how organizations develop and execute business strategy enabled by IT. The first era was data processing, next came information systems, and finally knowledge management. One sees how this evolution aligns with SAP's continuous improvement program. The desired outcome for IT to improve business efficiency has stayed consistent through the years. However, the delivery of value-producing systems has not been easy to achieve until we finally reached this knowledge management era. The state of art at the time R/3 was being developed was not in keeping with that early vision.

Now, we fast forward to today and can see that our vision goes beyond enabling business and sees IT as an almost equal partner in effecting business efficiency. Today's worker is now a knowledge worker enabled by Web-based flexible tools and technologies. These tools provide nearly instant information about the business problems they are working with. But with the incredible efficiency SAP can provide comes a heavy burden on infrastructure complexity. The systems requirements for SAP are significant in terms of IT architecture, development architecture, and security infrastructure. In fact, I would maintain that embedded into every aspect of the infrastructure is now a component of security specification that must be addressed. Unfortunately, we still see many occasions where security is the appendix of the infrastructure plan. Security is often relegated to an after-thought that only gets emergency attention when an event occurs, a question of senior management is asked, or an audit drives a specific change. It is the rare organization that has an embedded active security-thinking culture.

Security infrastructure as an embedded part of the IT culture has yet to be recognized in the mainstream. However, when you consider the initiatives being

addressed in corporations, institutions, and governments throughout the world, you begin to understand the strategic intent in evolving security. In nearly every conference on technology in the SAP and out of the SAP space there is a topic on security. And, now, SAP NetWeaver technology has evolved to include the major SAP components necessary to implement the full life cycle of security infrastructure. While IT enables business, security enables IT, and hence security is the underlying foundation to the business enablement.

With IT organizations yet to adapt to this mind-set, the challenges are even greater. Most IT organizations are classically stove-piped and hence the skills and training associated with these stovepipes are yet to evolve. Even worse, often an organization creates project teams that may tax the stove-piped security group with a part-time representative. When I speak with young engineers across the organization, however, they seem to realize the change that's happening and are struggling to help their leaders make the right investments and reorganize to face the change. I challenge management to bring these facets out in the open and create enabling organizations that put the security mind-set at the forefront. It's no longer a cliché to say that security is everyone's responsibility. SAP has laid a foundation for this. In each aspect of SAP's NetWeaver use-case scenarios lies a security layer. SAP describes these as usage types, which determine the intended purpose of a system or sub-system. They are available by installing and configuring collections of software components.

Figure 1.1 presents NetWeaver as a collection of components that meet different needs up and down the integration stack.[2] It is important to recognize that today SAP NetWeaver is more than just a collection of components; it is an open technology platform which offers a comprehensive set of technologic capabilities that are natively integrated to support the needs of IT organizations worldwide. By reviewing the full gamut of capabilities one arrives at IT Scenarios and IT Practices that I refer to as use-cases.

Figure 1.1 SAP NetWeaver Usage Type Component Collection

IT Practice	IT Scenarios			
Enabling User Productivity	Enterprise Portals, Enabling Collaboration, Dashboards	Business Workflow	Mobilization	Enterprise Knowledge Management
Unification of Data	Master Data Synchronization	Master Data Consolidation	Central Data Management	Enterprise Data Warehousing
Business Support	Enterprise Reporting	Business Planning	Analytical Modeling	Enterprise Data Warehousing
Process Fulfillment	Enabling Business Workflows	Enabling eCommerce	Business Process Management	Business Workflow
Customized Development	Application Development	Applications Test & Delivery	Application Integration	Enabling Platform Interoperability
Unified Life-Cycle Management	Software Lifecycle Management	Systems Development Lifecycle	Solution Management Framework	SAP NetWeaver Operations & Design
Governance and Security	Authentication and Single Sign-On	Integrated User and Access Management	Segregation of Duties	Risk Management
Consolidation	Enabling Platform Interoperability	SAP NetWeaver Operations & Design	Master Data Consolidation & Unification	Enterprise Knowledge Management
Enterprise Services	Enabling Services	Open Standards	SAP NetWeaver Operations & Design	Solution Management Framework

IT Scenarios identify how one uses SAP NetWeaver to solve specific business problems. This is accomplished through deployment of the integrated IT scenarios in a way that does not disrupt existing business operations. IT practices look at the overall SAP NetWeaver platform as a strategic investment. One views the usage framework vertically and determines the options to focus on critical business issues rather then specific business problems addressed by tactical scenarios. This flexibility is the power of SAP NetWeaver.

SAP recommends that each practice be broken into one or multiple IT scenarios, providing organizations with a process-oriented approach to making best use of NetWeaver. By implementing IT scenarios, customers can adopt core functionality of SAP NetWeaver in incremental phases. The aim of IT scenarios is to help customers, partners, and independent software vendors (ISVs) install and operate SAP NetWeaver, to run business applications (custom-built and packaged applications), or to implement a defined IT goal like migrating to the services architecture. Focusing on the flow of activities rather than on the nature of the involved components, IT scenarios are collections aimed at resolving specific business area challenges.

The best way to see these IT practices and IT scenarios is with the SAP NetWeaver Technology Map.[3]

The SAP NetWeaver Technology Map

In Figure 1.1, each IT practice is on the left, with its associated IT scenarios to the right. Usage types describe how installations of SAP NetWeaver are used, and which capabilities each offers to the overall IT landscape. By providing installation and basic configuration support for SAP NetWeaver systems, usage types provide the groundwork to run IT and business scenarios. Usage types make system landscape planning easier by determining how capabilities provided by SAP NetWeaver can be deployed and activated in a SAP NetWeaver system. In addition, configuration will be simplified by offering configuration templates for usage types and IT scenarios. Usage types were introduced with SAP NetWeaver 7.0. Each scenario or practice has a security implication. Each instantiation comes with its own unique set of questions, technologies, and considerations for implementation and architecture.

As an organization implements a new component or scenario, the development cycle used to design, create, test, and deploy must adopt their design and testing methodology to ensure compliance. There are a host of tools and processes available for this. This book, then, is to be a model for highlighting the SAP technologies available for implementing and institutionalizing security into the technology plans and implementations throughout the industry.

Security can no longer be the afterthought for implementations. I contend that as an afterthought, it is more costly to implement and retrofit. But as a key component in the early planning of any implementation security, security considerations are an equal partner in the design. A simple example of this shift is the following. Let's take

a mythical company, Superior Marbles Inc. Superior Marbles has successfully deployed SAP and is using the system to manage its assets. A key aspect to many assets in a firm is location. And, with assets that are used by the average worker, tracking can be quite difficult. Every two or three years an asset such as a PC or cell phone may need to be replaced or upgraded. Also, work or home office locations for these devices must be tracked. Finally, when an employee leaves of the assets must be collected and accounted for. So, in this example, let us consider the Superior Marbles sales team. The sales force often has a personal data assistant (PDA), a laptop, a printer, and so on. So in a firm with 50 sales people we are quickly dealing with at least 150 line items to track.

The capital acquisition is an easy entry into SAP by the purchasing/receiving organizations, but when the asset is delivered it is no longer easy to track. Typically, inside SAP the tracking is at a cost center/departmental level. But, with a useful kiosk through the Web, enabling the sales team to self manage the assets would prove extremely useful. So, an extension from the SAP database to an applet available to end-users (the sales people) over the Web will be our project. Many technologies are in play for this project. How will they securely log in? What will be presented to them and how will the data exchange occur back into SAP?

One can envision tackling the project via the typical analysis/requirements development process. But where are the security considerations determined and discussed with the user? They often aren't. It's left to IT network people, IT architects, and the developers to build on the basic requirements and ensure security. Even worse, there are times when audit concerns are missed until an actual audit, which can reveal additional shortcomings. So, the corrected approach is to address with the users the complete life cycle for the application and secure the application and its data. Having proper requirements specifications for the development team removes the ambiguity. And, better still, during audits these specifications are part of the development record and often this kind of data serves an important purpose as part of the catalog of documents used in building the application. So, then, what are the technologies that one must be concerned with in deploying an application within the SAP framework?

There are three key underlying concepts to all of the security infrastructure layers. These are data integrity, user access, and user authorization. Simply put, how is the data in the system ensured, how do users gain access, and what can users do with that access? The concepts associated with securing the infrastructure and applications will address these three key areas.

Scope

The scope of this discussion will be focused on four overlying security technologies that specifically encompass SAP. There are a host of certified for NetWeaver non-SAP, such as Microsoft's BizTalk framework that complement SAP; however, these are out of scope for this book. It is hoped that through a study of the components and considerations of the SAP technologies extension to the non-SAP is possible. The same considerations will be consistent across the infrastructure independent of the specific technology. Thus, we will focus on both ABAP and Java Web Application Server 7.0, Governance, Risk and Compliance (GRC) and the typical backend infrastructure foundations UNIX/Oracle. We do not mean to exclude specific, relevant technologies such as SQL Server or Linux, but we believe extensibility is appropriate and we also find in the main that UNIX/Oracle still appear to have the lion's share of systems in an SAP installation. Thus, if you are working in a heterogeneous landscape the concepts outlined here will still apply.

NetWeaver Web Application Server

SAP NetWeaver 7.0 provides an open integration and application platform and facilitates the implementation of Enterprise Services Architecture (see Figure 1.2). Both ABAP and Java are fully supported in SAP. Sizing considerations and architecture plans should be considered in order to determine the best model for implementing these stacks. While integrated ABAP/JAVA Web AS on the same server is possible, it is recommended to have separate hardware (application server) in either virtual or physical modes for the ABAP Web AS and the JAVA Web AS. Highlighted in the following sections is an overview of the J2EE Web AS and the ABAP Web AS feature, functions, and security insights.

Figure 1.2 NetWeaver Application Server Architecture

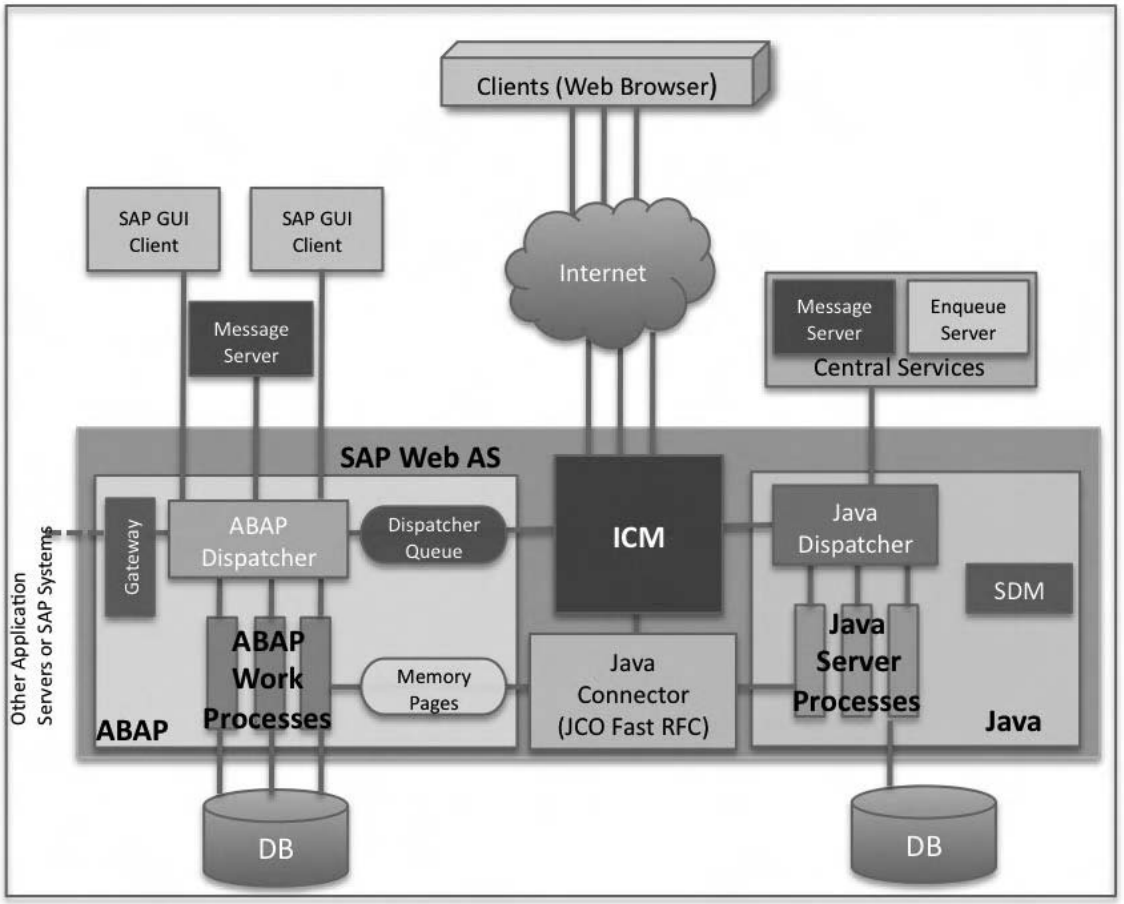


Figure 1.2 describes the combined ABAP and Java Web Application Architecture. Yellow Represents ABAP components and Green is Java. As mentioned previously, if you can afford it, the advantages to installing separate Java and ABAP engines outweigh the cost. For example, the technical patch requirements are more complicated and if patching one or the other service is necessary, with separate installations the other stays up while one is being patched. The Internet Communication Manager (ICM) is independent from the ABAP and JAVA stack but is installed with the ABAP application server. The ICM determines how to forward Web traffic requests. Each engine has a dispatch queue and the Java connector shown is an independent component but a function of the Java engine. It enables communication between ABAP and Java.

Client options are SAP GUI or Web Browser. The ICM is the Internet Communication manager which sets up the connection to the Internet for browser-based communications. The ICM process uses threads to parallelize the load that come through it. It can process both server and client Web requests. It supports the protocols Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), and Simple Mail Transfer Protocol (SMTP). The dispatcher distributes the requests to the work processes. If all the processes are occupied the requests are stored in the dispatcher queue.

The ABAP work processes execute the ABAP code and the Java Server processes the Java code.

The Gateway makes the Request for Comments (RFC) interface between the SAP instances available within an SAP System and beyond system boundaries. Message servers exchange messages and balance the load in an SAP System.

ABAP WEB AS 7.0

System security functions that apply specifically for SAP Web AS ABAP are Trust Manager and Security Audit Log. Trust manager is the tool to use when using public-key technology with the SAP Web AS ABAP server. Use the Security Audit Log to keep track of security-related events on the SAP Web AS ABAP server. Events such as unsuccessful log-on attempts, starting of transactions or reports, or changes to user master records can be recorded and analyzed. Secure storage is part of the SAP Web Application Server ABAP and is used by SAP applications to store the passwords used for connecting to other systems. The passwords are stored encrypted. As a result they cannot be accessed by unauthorized users.

Establishing solid trust relationships is vital to the success of business processing. This becomes paramount with today's mobile knowledge worker that transcends corporate bounds and works from anyplace. Therefore, many applications in SAP Systems rely on the use of public-key technology to establish the trust infrastructure that is necessary for successful business relationships.

SAP Systems support the use of an external security product using the Secure Store and Forward (SSF) mechanism. By using SSF, applications can support the use of digital signatures and document encryption in their processing. At start-up, each SAP System is supplied with a public-key pair, which includes a public-key certificate that is stored in its own system Personal Security Environment (PSE). The SAP System can therefore produce its own digital signatures using the public-key

information contained in its system PSE. Other systems can then verify the system's digital signature, which guarantees the integrity and authenticity of a document that has been digitally signed by the system. With the SAP Web AS, a single login by a user enables the system to authenticate the user through other subsystems using the digital signature provided with the log-on ticket. Lastly, The SAP Web AS supports the Secure Sockets Layer (SSL) protocol, which provides for authentication between communication partners and encrypted communications. In this case, the application server must also possess a public and private key pair to use for the SSL communications.

The Security Audit Log is designed for security and audit administrators who wish to have detailed information on what occurs in the SAP System. By activating the audit log, you keep a record of those activities you consider relevant for auditing. You can then access this information for evaluation in the form of an audit analysis report.

The SAP Web AS ABAP communicates with its communication partners using various protocols. The primary protocols used are Dialog (DIAG), RFC, and HTTP. The security mechanism for managing these protocols is either Secure Network Communication (SNC) or SSL.

J2EE WEB AS 7.0

SAP NetWeaver 7.0 provides an open integration and application platform and facilitates the implementation of the Enterprise Services Architecture. The Java SAP Web Application Server provides complete user management services called a User Management Engine or UME, the Universal Description Discovery and Integration or UDDI and data base integration facilities. By default, UME is set upon install.

The purpose of the UME is to provide central user administration for all applications developed using Java. The UME is completely integrated into SAP Web Application Server Java as a service and is used as the default user store. The UME itself administers users and uses databases, directory services, or the SAP ABAP user administration to store the data. In the UME, the words *data sources* are used to refer to repositories for user data.

To display the active user store, select a Server in the Visual Administrator. In the Security Provider service, select **Runtime → User Management**, and choose

Manage Security Stores. If it is grayed out, you have to go to **Change Mode**. If Activate User Store is inactive for a user store, this means that the user store that you have just chosen is already active. If you want to use UDDI instead of the default user store UME, you can use the described method to change this by choosing **Activate User Store** for the UDDI user store.

UME Installation Options

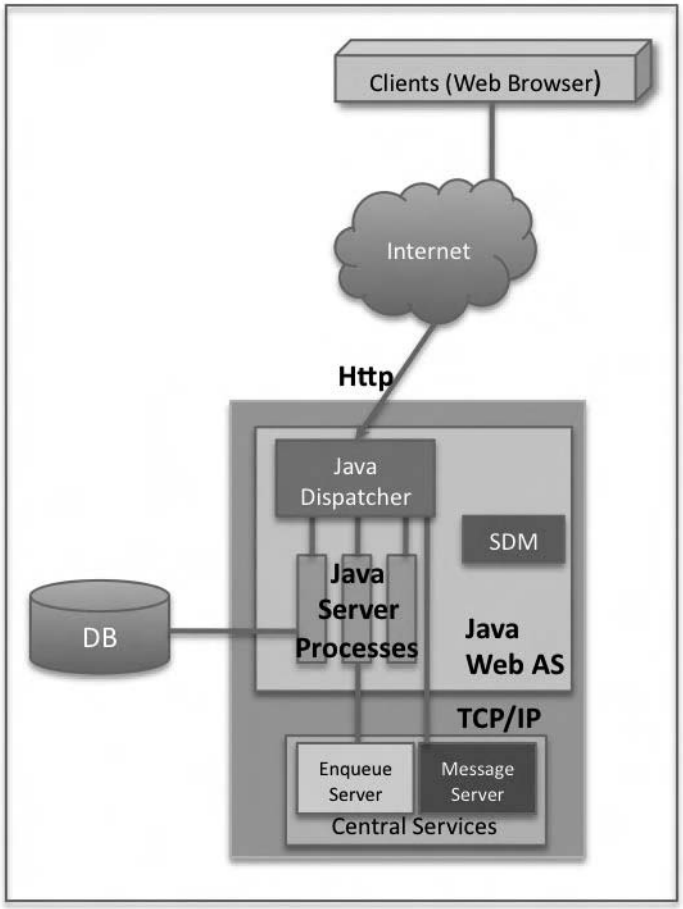
During the installation of an SAP Web Application Server (SAP Web AS), you can select the following options for setting up the UME:

- **SAP Web AS Java (without ABAP)** The UME can be configured so that the ABAP user management of another SAP Web Application Server ABAP is used. The UME can be configured so that the database of this SAP Web Application Server Java is used to store user data.
- **SAP Web AS ABAP + Java** The UME is configured so that the ABAP user management of this SAP Web Application Server is used. By default, you have read-only access to the user data in ABAP user management from the UME.

The communication between the UME and the ABAP user management is performed with the SAPJSF user. After an installation, this user has the ABAP role SAP_BC_JSF_COMMUNICATION_RO, which provides read access from the UME to the ABAP user management. You can obtain write access by adding the role SAP_BC_JSF_COMMUNICATION. SAP recommends the role SAP_BC_JSF_COMMUNICATION_RO for this user. You can only configure the use of a directory service as the data source later. In this case, it is recommended that you use the database as the data source for user data during the installation Administration of Users (UME with ABAP User Management as data source) ABAP Users: transaction SU01, ABAP authorizations and roles: transaction PFCG, Java authorizations and roles (UME roles, security roles): Visual Administrator and UME administration console. If you are using an SAP Enterprise Portal in this environment, the user administration is controlled using the portal.

The Java dispatcher receives the client request and forwards it to the server process with the lowest capacity usage. If there is already a connection to the client, the request goes to the server process that processes this client (see Figure 1.3).

Figure 1.3 Java Web Application Server Architecture



To operate the J2EE Engine, the following services must be active in the HTTP service tree (transaction SICF):

- **/sap/public/icman:** The ICM uses this service to forward requests to the J2EE Engine.
- **/sap/public/icf_info** supplies the Web Dispatcher the details of log-on groups, server load, and so on.

These services must be activated so that the SAP Web dispatcher and the ICM can forward the request correctly. If these services are not active, you have to activate them in transaction SICF.[4]

The Web Dispatcher is the central access point from the Internet into the SAP System. The Web dispatcher has to decide to which SAP Web AS it will send each incoming request. For each incoming HTTP request, the ICM must decide whether it should forward the request for processing to the ABAP engine or to the J2EE engine. This decision is made using the URL prefix. A separate protocol is used for the communication between the ICM and Java Dispatcher. The ICM can be set up so that the communication with the J2EE Engine is SSL-encrypted. If the ICM receives an HTTPS request, it decodes it. If it determines from the URL that the request should go to the J2EE Engine, there are various communication options. You can set whether the request should be SSL-encrypted, before it is forwarded to the J2EE Engine. You can do this in the following ways:

- Do not encrypt the request: The request is sent to the J2EE Engine with the protocol described above via TCP sockets.
- Encrypt the HTTPS request again: All requests that arrived as HTTPS at the ICM are SSL-encrypted again, before they are sent to the J2EE Engine.
- Encrypt all requests: Regardless of whether the request was HTTP or HTTPS, it is SSL-encrypted, before it is sent to the J2EE Engine.

The ICM is configured for communicating with the J2EE Engine using an icm profile parameter.[5]

The Software Deployment Manager (SDM) is an integrated directory of SAP software components in the library. The SAP Web AS engine includes the Universal Description, Discovery and Integration (UDDI) Business Registry. This is a global, public, online directory that gives businesses a uniform way to describe their services, discover other companies' services, and understand the methods necessary to conduct e-business with a particular company. As a key element of the framework that makes Web services a reality, the UDDI Business Registry is an implementation based on the UDDI Specifications.[6]

UDDI has been around for several years initially driven by IBM and SAP adopted it in 2001. Unfortunately, the incredible power of UDDI offers significant concerns in the security and change management space. It's vital to have a test program that actively manages in this arena. Today's Java development world still lacks rigorous change control and tracking. As a result, while Java development projects facilitate rapid delivery through component reuse and ease of programming, it can be a two edged sword. Its important to understand the building blocks and

risks associated with these in order to have an active program that certifies use of programs and components.

The J2EE Engine can communicate with its communication partners using several different protocols. The primary protocol used is HTTP, however, P4, which is the protocol to use for RMI, as well as the protocols LDAP, ODBC, and telnet are also supported. SAP documents the protocols and security methods in the online documentation. Table 1.1 lists this information.

Table 1.1 Protocols and Security Methods

Protocol	Security Mechanism	Comment
HTTP	SSL	SSL provides for authentication, integrity, and privacy protection.
P4	SSL	P4 is the transfer protocol for RMI and when using the Visual Administrator. P4 supports HTTP tunneling and can also be used with proxies.
LDAP	SSL	You can use an LDAP directory server as the persistency layer for the UME user store.
RFC	SNC (Secure Network Communications)	SNC is a SAP-proprietary layer used with the NI protocol.
ODBC	driver-dependent	Used to connect to the database.
Telnet	Virtual Private Network	You can use telnet for remote administration.

Additional system security functions for SAP Web AS Java include Key Storage service, Managing protection domains, Secured Web service, Application specific secured storage, File System secured storage, and Managed log-in sessions.

The Key Storage service of the J2EE Engine enables you to manage certificates and credentials on the server; you can also use it to generate keys and certificates. Application specific secured storage is related to this area. These keys and certificates can be used for encrypting, identification, and verification. The Key Storage entries are stored in a distributed database and can be assigned particular access rights. The service is compatible with the Java Cryptography Architecture.[7]

Protection domains enable you to manage system resources. This enables you to make access control decisions. You can add new categories of permissions that are supported by the J2EE Engine.

With secured Web services a user (or other client) sends a document to a server using the Simple Object Access Protocol (SOAP), which is then sent over the network using the HTTP protocol. Therefore, to secure this communication, one can use the SSL protocol, which is supported by the J2EE Engine. What you must ensure is that you secure the transmission and have proper authorizations for processing such documents. There are several mechanisms available on the J2EE Engine, which include securing the communications, authenticating the client, and providing for authorizations. The J2EE Engine implements the *Java Authentication and Authorization Service (JAAS)* standard to support various authentication methods. This enables you to choose the required authentication mechanisms for your applications.

Applications running on the J2EE Engine can either use declarative or programmatic authentication. Both types of authentication rely on the same underlying technology: log-in modules and log-in module stacks. Programmatic authentication additionally uses authentication schemes. SAP ships log-in modules and authentication schemes to support various authentication mechanisms.

Protection domains enable you to manage system resources. This enables you to make access control decisions. You can add new categories of permissions that are supported by the J2EE Engine.

The SAP Web AS Java stores security-relevant information encrypted in a file in the file system. Because the cryptographic software needs to be deployed after the installation, you first need to activate the secure storage in the file system to have this information stored in encrypted form. Alternately, the information is encoded using 64 bit encoding.

J2EE Engine associates a security session object to the thread of control of each authenticated user for a login. The security session is recognized by the cluster element it is created in. It is also has an associated signed certificate by the cluster element that identifies the security session. It can be transferred by protocols that cannot or do not want to maintain client sessions on their own.

Backend: UNIX/Oracle

Today's SAP infrastructure offers incredible flexibility. From single-system landscapes to multisystem heterogeneous environments, SAP has the capability to manage and execute in these frameworks. Any landscape planning must take into account

the intended purpose for the initial and postproduction architecture. As well, the organizations hardware familiarity and strategic plans are also critical to successful planning. Finally, a maintainable environment that can be understood and managed by all IT administrators is also a priority.

Infrastructure team resources are given a lot of work today. And, often this work comes with conflicting priorities. The flexibility for choosing the right backend technology offers another project for consideration by the already over-worked infrastructure team. It is important, therefore, to select a maintainable infrastructure to minimize additional burden on the infrastructure team. But, with the right level of planning and documentation selecting a maintainable infrastructure should be easy. A key to making the decision on backend infrastructure is sizing. SAP together with its partner vendors and ISVs can offer a good deal of help in the sizing and planning for the infrastructure decision. With the onset of the NetWeaver usage type Scenarios, it is important to develop an adaptable infrastructure that can be extended at the lowest cost. Initial hardware costs often pale in comparison to the actual operating costs and impacts to administrators. There are new tools available from Oracle that aid in system management. As of basis release 7.00 SP12, DBACOCKPIT is the new central database administration tool. It is a representative monitoring transaction. This now offers a Unified framework with a consistent look and feel for all SAP supported DB/OS platforms. DBACOCKPIT contains former ST04 (for Performance), DB02 (for Space), and planning calendar (DB13) functions and includes several new monitors (particularly for Oracle 10g) with RAC monitoring now embedded. Monitoring and administration of remote Oracle and non-Oracle databases (both ABAP and non-ABAP systems) is also possible via DB MultiConnect. The former transactions ST04, DB02, DB13 (for Jobs), and others are still available but have been renamed to ST04OLD, DB02OLD, DB13OLD, etc., and will become unnecessary in future releases.

When connecting to the database, the J2EE Engine and the applications deployed on it authenticate themselves by means of a user name and a password. They are specified only once, when the DataSource that is used to provide the database connection is created. The DataSource is initialized with the supplied credentials and uses them for the authentication of all physical connections that it provides.

You can use one of two options for database connectivity. You can use the default DataSource. With this source you can connect to the system database in which the J2EE Engine stores its information. Alternately, you can register a new DataSource to connect to another database that your application uses.

Governance, Risk, and Compliance (GRC)

In 1982 the Defense Science Board (DSB) Task Force examined why the **Department of Defense** (DoD) continued to experience significant cost overruns and schedule delays on major weapon system acquisitions. The resulting DSB report identified a lack of a systematic approach to managing technical risk as the primary cause of system cost overruns and deployment delays.

The DSB noted that although cost overruns and schedule delays often manifested themselves during full-scale production, the origin of most production problems stemmed from design risks.[8] As a result, the DSB recommended that the DoD develop a systematic approach for identifying, understanding, and managing technical risk throughout a weapon system's life cycle, with specific emphasis on managing design risk.

While initially developed for Weapons System, the documentation from the DoD has been extended through the years and applied to a plethora of technical systems development outside those on which the DoD initially focused.

The outcome of the 1982 DSB study was the issuance of DoD 4245.7-M, "Transition from Development to Production,"[9] in September 1985. DoD 4245.7-M decomposes each phase of a weapon system's developmental life cycle into discrete steps, and, in template form, identifies potential risks and provides recommendations for reducing those risks. Another critical work product from the DoD is the "Risk Management Guide for DoD Acquisition."[10] In government projects these documents often go hand in hand.

The focus of other DoD risk discussions and articles on the subject go on to marry contracts with risk assessment, that is, how government contract types are determined and used in control and management of risks. It is not our intent to discuss the issues and options of Federal Accounting Regulations (FAR) supplements or practices as they relate to risk. But, rather it is our intent to create a framework to apply in and out of the government and on projects both large and small. It is up to the user to determine the risk framework. That framework can be the foundation for assessing and scoping the risk program in the project and the design process and decisions for what to implement and how. I hope to provide a solid foundation for understanding risk science. As it relates to the overall subject of security in general, I will propose an alternate means for thinking about risk. As in determination of security implications up front in design, risk determination, too, should be made up front in program or project planning. They go hand in hand.

Establishing a risk-conscious culture can lead to far better quality systems implementations and cost control.

The Risk Management Guide states that each risk has three components. These components are:

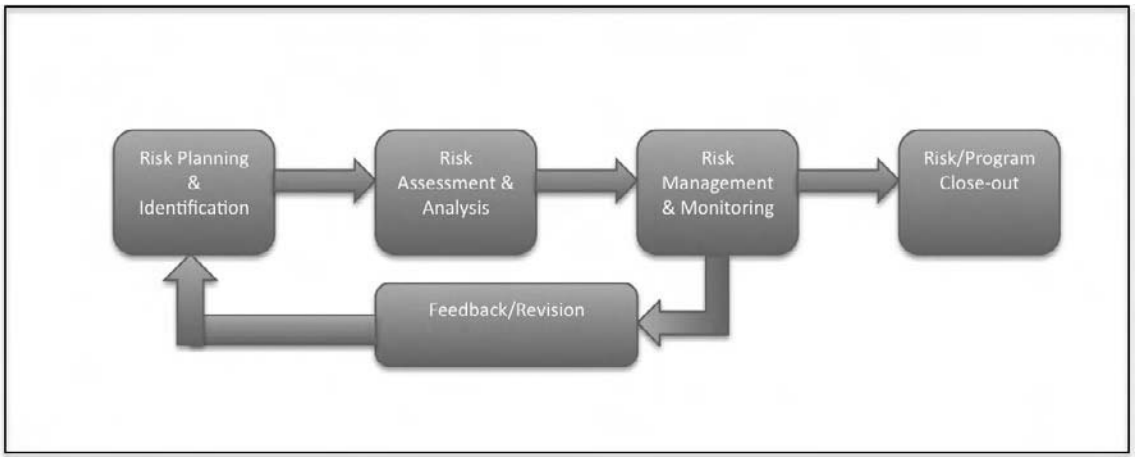
- A future root cause
- The probability of the future root cause occurring
- The consequence/impact if the root cause occurs

In distinguishing between risk management and issue management risks are events yet to happen. They have future consequences, and can be "closed" only after successful mitigation through avoiding, controlling, transferring, or assuming the risk. Issues are current problems and/or challenges with real or near real-time consequences, and can be closed within shorter windows as they complete. Often risk closure is only possible at the end of a project or program when all mitigations are proven or in force.

At NASA we use the DoD risk management process, as outlined in the DoD "Risk Management Guide for DoD Acquisition" referred to above for many of our programs and we are additionally involved in further improvement of the science of risk management. In 2000 NASA commissioned the University of Virginia's Center for Risk Management of Engineering Systems, directed by Dr. Yacov Y. Haimes, to develop a five-year roadmap that identifies the activities required to meet NASA's long-term corporate goals. The purpose of the Capstone effort was to locate and analyze different methodologies that could be incorporated into this plan. The plan was presented in 2001.[11]

Several disasters in NASA's past caused a top to bottom assessment of how to improve the culture at NASA. As a result of the many identified improvement recommendations a better focus on risk management was created. This risk management process includes risk planning, assessment (identification and analysis), handling, and monitoring steps with feedback from risk monitoring and documentation for all process steps as illustrated in Figure 1.4.

Figure 1.4 A Typical Risk Management Process



Risk Planning & Identification involves developing and documenting a systematic and comprehensive strategy and methods for identifying and analyzing risk issues, developing and implementing risk handling plans, and documenting the overall risk management process. The identification piece is the initial examination of all program/project areas for potential risks to be fed to the next phase for formal documentation and mitigation management.

Risk Assessment & Analysis involves examining each identified risk issue and validates its applicability in scope for the program/project. Each risk level is identified as well.

Risk Management & Monitoring involves the continuous tracking of active risks and potential additional risk during the program. Levels are continuously assessed and validated (up or down) and closure recommendations can also be made.

Risk/Program Close-out involves the closure of individual risks as appropriate; when the program is complete a risk close-out is conducted for all remaining open items in the event the program is moved to operation/maintenance.

Feedback/Revision involves the continuous improvement of the process and extension of new risks as they are identified for proper documentation.

In getting a program or project started, the critical task in *Risk Planning & Identification* is agreeing on the risk plan and methodology. Determining risk items and scope is covered in this arena. As the general requirements of the technical challenge to be implemented unfold, a thorough analysis must be made. A risk matrix is the proper place to start once consequences and impacts are determined. Typically

the probability for an item's occurrence is factored against the consequence to yield impact values of between 1 and 5. Table 1.2 lists some generic risks such as cost overrun, and so on. In the even cost overrun were to likely cause project cancellation, the risk might be considered High. Or, alternately should cost overrun drive a descoping event, the risk might be considered Low.

Table 1.2 A Sample Risk Matrix

Consequence	Impact	Impact	Impact
Cost Overrun	Descope	Extend Schedule	Project Cancellation
Schedule exceeded	Increase Cost	Descope	Project Cancellation
Requirement mismatch	Replan	Rescope	Revise Project

It is in collecting and discussing how to rank these impacts against a consequence that the science of risk management is at its best.

On a typical project, a comprehensive risk evaluation might be used to both screen and tailor the items included on each piece of documentation. Several inputs can be used to perform risk identification, including the following:

- The project organization
- The project budget
- The project schedule
- Lessons learned from other projects
- Project performance requirements
- Information about key business processes and rules
- Auditability requirements
- Initial segregation of duty and execution requirements

For each discussion comes mitigations aimed at ensuring the risks are fully understood, well managed, and mitigated. In SAP's GRC offering on security we have a product that enables administrators and users to define policies or rules, and enforce these policies through the provisioning of services. SAP GRC Access Control delivers a comprehensive, cross-enterprise set of Access Control facilities that enables agencies and companies alike to define and monitor SOD enforcement, role and