


Risk Matrix

Information Technology Risk Matrix



Risk assessment is a process of estimating a risk score to be associated with each auditable technology. Risk assessments are typically undertaken to focus attention on significant audit areas, to allocate scarce audit resources to the most important audit areas, and to help with key audit prioritizing decisions such as frequency, intensity and timing.

The criteria used to assign risk scores include:

- Date and results of the last audit
- Financial exposure
- Potential loss and risk
- Requests from management
- Major changes to environment
- Corporate reliance on technology

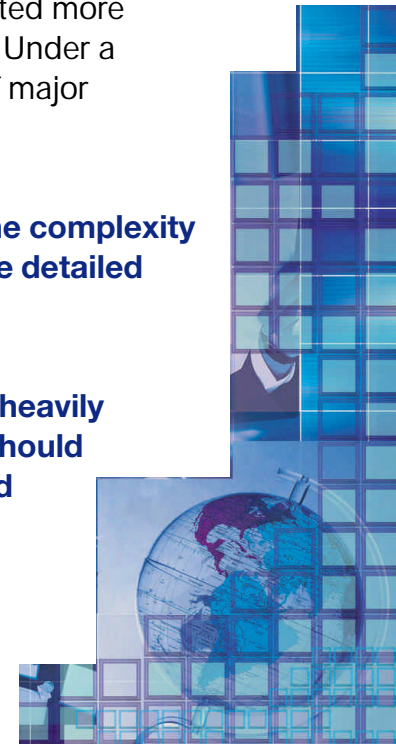
This points out that the riskiness of a specific auditable technology is based on multiple factors. Additionally, the risk score alone may not be a sufficient basis for making an audit planning decision. It may be necessary to factor in the cost of carrying out the audit as it relates to the relative risk an organization is willing to assume.


The general opinion, with respect to **Audit frequency**, is that riskier technologies should be audited more frequently. The matrix is a guide that should be used in conjunction with a conditional audit frequency approach. Under a conditional audit frequency approach all key technologies are monitored for signs of major changes. Examples of major changes include significant upgrades, reconfigurations and the addition of a large number of users.

Audit intensity should be determined by assessing the qualifications of the resources and the complexity of the technology. Generally, the more complex the technology, given the same level of staff skills the more detailed the audit.

Audit timing is another component to be considered during planning. Again, audit planning is heavily dependent upon resource availability. A variety of approaches have been used to determine when audits should be scheduled. Fixed time audits are based on the assumption that there are fixed times that are best suited to conduct the audit; whereas, random timing audits are more unpredictable and may be used to motivate IT personnel to maintain their controls and procedures at reasonable levels.

Audit frequency, intensity, timing and resources are key components that should be considered when using the Technology Risk Matrix.





Risk is the potential for loss to an enterprise due to error, fraud, inefficiency, failure to comply with statutory requirements, or actions which bring disrepute to the entity. Risk is a synonym for all the adverse outcomes that the organization wishes to avoid. Risk is a function of the probability that such consequences will occur, their magnitude, and their imminence.

Technology Risk Components:

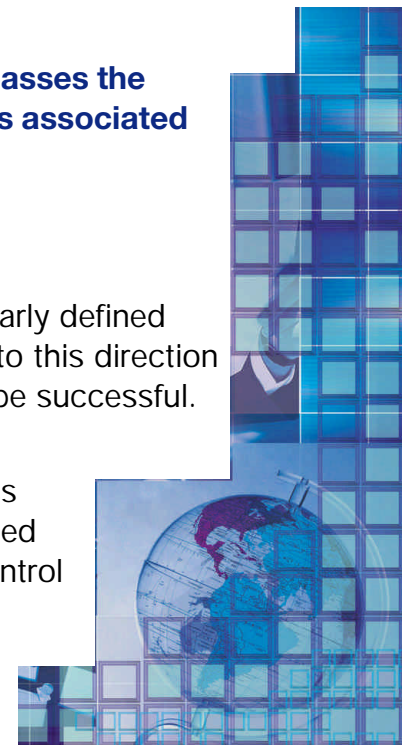
Integrity Risk – risks associated with the authorization, completeness, and accuracy of transactions as they are entered into, processed by, summarized by and reported on by the various application systems deployed by an organization.

Relevance Risk – the usability and timeliness of information that is either created or summarized by an application system is the risk associated with not getting the right data/information to the right person/process/system at the right time to allow the right action to be taken.

Access Risk – risk associated with inappropriate access to systems, data or information. It encompasses the risks of improper segregation of duties, risks associated with the integrity of data and databases, and risks associated with information confidentiality.

Infrastructure Risk:

- **Organization Planning** – the definition of how IT will impact the business are clearly defined and articulated. It is important to have adequate executive level support and buy-in to this direction and an adequate organizational (people & process) plan to ensure that IT efforts will be successful.
- **Application Deployment** – ensuring that application systems meet both business and user needs. This process ensures that any change to systems, whether purchased or developed internally, follow a defined process that ensures that critical process/control points are consistently followed.





Infrastructure Risk: (cont.)

- **Logical Security** – ensuring that the organization adequately addresses access risk by establishing, maintaining and monitoring a comprehensive system of internal security that meets management's policies with respect to the integrity and confidentiality of the data and information within the organization.
- **Computer Operations** – ensuring that information systems and related network environments are operated in a secured and protected environment as intended by management. Additionally, ensuring that information processing responsibilities performed by operations personnel are defined, measured and monitored.
- **Disaster Recovery** – ensuring that adequate planning has been performed to ensure that information technologies will be available to users when they need them.





IT Risk Matrix by SCORE

Company Name

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DESCRIPTION	Risk Score	2006	2007	2008 - 2012
1	APPLICATIONS	Oracle Financials	Financial Management	38.0			x
2	APPLICATIONS	PeopleSoft HR Payroll	Human Resource Management	38.0			x
3	APPLICATIONS	AIM	EMS Billing Application	35.0	x		
4	OTHER AUDITS	Email Usage & Control	Email Usage, Archival, and Legal	33.0	x		
5	PLATFORMS	AIX Server - Oracle Financials	Oracle Financials	33.0			x
6	PLATFORMS	WIN Server - W2K3APPS14PT	PeopleSoft HR Payroll	33.0			x
7	PLATFORMS	WIN Server - W2K3APPS13PT	PeopleSoft HR Payroll	33.0			x
8	PLATFORMS	WIN Server - W2K3APPS15	County Attorney Applications	32.0	x		
9	APPLICATIONS	Risk Management	Worker's Comp. & Child Support	32.0	x		
10	PERIMETER	Firewall(s)	Perimeter Firewalls	32.0	x		
11	DATABASE	SQL Server 2000 - W2K3DB02	Risk Management Database	31.0		x	
12	APPLICATIONS	Chevin Fleet Management	Government Fleet Management	31.0		x	
13	DATABASE	SQL Server 2000 - W2K3DB05	PeopleSoft HR Payroll Database	31.0			x
14	OTHER AUDITS	System Development	Application Development Controls	30.0		x	
15	DATABASE	Oracle DB	Oracle Financials Database	30.0			x
16	APPLICATIONS	IMS	Inmate Management System	30.0		x	
17	OTHER AUDITS	Disaster Recovery	DR Business Continuity Plan	29.0			x
18	APPLICATIONS	Cashier	Payment Processing to Oracle	29.0		x	
19	DATABASE	SQL Server 2000 - W2K3DBDEV02	Authorization Manager Database	28.0		x	
20	OTHER AUDITS	Active Directory	Network Authentication	28.0			x
21	DATABASE	SQL Server 2000 - W2K3DB01	Fleet Management Cashier Database	27.0			x
22	OTHER AUDITS	Data Center Controls	Datacenter Security & Environmental	27.0			x
23	PLATFORMS	WIN Server - W2KAPPS05	Revenue Commission (CARS)	27.0			x
24	OTHER AUDITS	Software Compliance	Software Audit	26.0			x
25	OTHER AUDITS	Change Control Management	Departmental Change Control Policy	25.0			x
26	PERIMETER	Penetration Testing	External & Internal Penetration Testing	25.0			x



IT Risk Matrix by CATEGORY

Company Name

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DESCRIPTION	Risk Score	2006	2007	2008 - 2012
1	APPLICATIONS	Oracle Financials	Financial Management	38.0			x
2	APPLICATIONS	PeopleSoft HR Payroll	Human Resource Management	38.0			x
3	APPLICATIONS	AIM	EMS Billing Application	35.0	x		
4	APPLICATIONS	Risk Management	Worker's Comp. & Child Support	32.0	x		
5	APPLICATIONS	Chevin Fleet Management	Government Fleet Management	31.0		x	
6	APPLICATIONS	IMS	Inmate Management System	30.0		x	
7	APPLICATIONS	Cashier	Payment Processing to Oracle	29.0			x
8	DATABASE	SQL Server 2000 - W2K3DB02	Risk Management Database	31.0		x	
9	DATABASE	SQL Server 2000 - W2K3DB05	PeopleSoft HR Payroll Database	31.0			x
10	DATABASE	Oracle DB	Oracle Financials Database	30.0		x	
11	DATABASE	SQL Server 2000 - W2K3DBDEV02	Authorization Manager Database	28.0		x	
12	DATABASE	SQL Server 2000 - W2K3DB01	Fleet Management Cashier Database	27.0			x
13	OTHER AUDITS	Email Usage & Control	Email Usage, Archival, and Legal	33.0	x		
14	OTHER AUDITS	System Development	Application Development Controls	30.0			x
15	OTHER AUDITS	Disaster Recovery	DR Business Continuity Plan	29.0		x	
16	OTHER AUDITS	Active Directory	Network Authentication	28.0			x
17	OTHER AUDITS	Data Center Controls	Datacenter Security & Environmental	27.0			x
18	OTHER AUDITS	Software Compliance	Software Audit	26.0			x
19	OTHER AUDITS	Change Control Management	Departmental Change Control Policy	25.0			x
20	PERIMETER	Firewall(s)	Perimeter Firewalls	32.0	x		
21	PERIMETER	Penetration Testing	External & Internal Penetration Testing	25.0			x
22	PLATFORMS	AIX Server - Oracle Financials	Oracle Financials	33.0			x
23	PLATFORMS	WIN Server - W2K3APPS14PT	PeopleSoft HR Payroll	33.0			x
24	PLATFORMS	WIN Server - W2K3APPS13PT	PeopleSoft HR Payroll	33.0			x
25	PLATFORMS	WIN Server - W2K3APPS15	County Attorney Applications	32.0	x		
26	PLATFORMS	WIN Server - W2KAPPS05	Revenue Commission (CARS)	27.0			x



IT Risk Matrix by YEAR

Company Name

I.D.	CATEGORY	AUDIT TECHNOLOGIES	DESCRIPTION	Risk Score	2006	2007	2008 - 2012
1	APPLICATIONS	AIM	EMS Billing Application	35.0	x		
2	OTHER AUDITS	Email Usage & Control	Email Usage, Archival, and Legal	33.0	x		
3	PLATFORMS	WIN Server - W2K3APPS15	County Attorney Applications	32.0	x		
4	APPLICATIONS	Risk Management	Worker's Comp. & Child Support	32.0	x		
5	PERIMETER	Firewall(s)	Perimeter Firewalls	32.0	x		
6	DATABASE	SQL Server 2000 - W2K3DB02	Risk Management Database	31.0		x	
7	APPLICATIONS	Chevin Fleet Management	Government Fleet Management	31.0		x	
8	OTHER AUDITS	System Development	Application Development Controls	30.0		x	
9	APPLICATIONS	Cashier	Payment Processing to Oracle	29.0		x	
10	DATABASE	SQL Server 2000 - W2K3DBDEV02	Authorization Manager Database	28.0		x	
11	APPLICATIONS	IMS	Inmate Management System	30.0		x	
12	APPLICATIONS	Oracle Financials	Financial Management	38.0			x
13	APPLICATIONS	PeopleSoft HR Payroll	Human Resource Management	38.0			x
14	PLATFORMS	AIX Server - Oracle Financials	Oracle Financials	33.0			x
15	PLATFORMS	WIN Server - W2K3APPS14PT	PeopleSoft HR Payroll	33.0			x
16	PLATFORMS	WIN Server - W2K3APPS13PT	PeopleSoft HR Payroll	33.0			x
17	DATABASE	SQL Server 2000 - W2K3DB05	PeopleSoft HR Payroll Database	31.0			x
18	DATABASE	Oracle DB	Oracle Financials Database	30.0			x
19	OTHER AUDITS	Disaster Recovery	DR Business Continuity Plan	29.0			x
20	OTHER AUDITS	Active Directory	Network Authentication	28.0			x
21	DATABASE	SQL Server 2000 - W2K3DB01	Fleet Management Cashier Database	27.0			x
22	OTHER AUDITS	Data Center Controls	Datacenter Security & Environmental	27.0			x
23	PLATFORMS	WIN Server - W2KAPPS05	Revenue Commission (CARS)	27.0			x
24	OTHER AUDITS	Software Compliance	Software Audit	26.0			x
25	OTHER AUDITS	Change Control Management	Departmental Change Control Policy	25.0			x
26	PERIMETER	Penetration Testing	External & Internal Penetration Testing	25.0			x



Risk Factor VALUES

Company Name

AUDIT TECHNOLOGIES	DESCRIPTION	Level of Government Reliance	Commercial vs. Internal	Last Audit	Internal Customer Impact	External Customer Impact	Potential Financial Exposure	Security Threat	Level of Admin Tasks	Major Recent Changes	Total
APPLICATIONS SECURITY & CONTROL AUDITS											
Oracle Financials	Financial Management	5.0	2.0	2.0	5.0	5.0	10.0	3.0	3.0	3.0	38.0
PeopleSoft HR Payroll	Human Resource Management	5.0	2.0	2.0	5.0	3.0	10.0	3.0	4.0	4.0	38.0
Risk Management	Worker's Comp. & Child Support	4.0	3.0	7.0	3.0	3.0	6.0	3.0	2.0	1.0	32.0
Chevin Fleet Management	Government Fleet Management	3.0	2.0	7.0	3.0	2.0	6.0	2.0	2.0	4.0	31.0
Cashier	Payment Processing to Oracle	3.0	3.0	7.0	3.0	2.0	6.0	2.0	2.0	1.0	29.0
AIM	EMS Billing Application	4.0	3.0	7.0	3.0	4.0	8.0	2.0	2.0	2.0	35.0
IMS	Inmate Management System	5.0	2.0	7.0	4.0	2.0	4.0	3.0	2.0	1.0	30.0
DATABASE SECURITY & CONTROL AUDITS											
Oracle DB	Oracle Financials Database	5.0	2.0	2.0	4.0	3.0	8.0	2.0	3.0	1.0	30.0
SQL Server 2000 - W2K3DB05	PeopleSoft HR Payroll Database	4.0	2.0	2.0	4.0	3.0	8.0	2.0	3.0	3.0	31.0
SQL Server 2000 - W2K3DB02	Risk Management Database	5.0	2.0	7.0	4.0	2.0	6.0	2.0	2.0	1.0	31.0
SQL Server 2000 - W2K3DB01	Fleet Management Cashier Database	3.0	2.0	7.0	3.0	-	4.0	2.0	2.0	4.0	27.0
SQL Server 2000 - W2K3DBDEV02	Authorization Manager Database	3.0	3.0	7.0	3.0	1.0	2.0	3.0	3.0	3.0	28.0
PLATFORMS/SERVER AUDITS											
AIX Server - Oracle Financials	Oracle Financials	5.0	2.0	2.0	4.0	4.0	8.0	2.0	3.0	3.0	33.0
WIN Server - W2K3APPS14PT	PeopleSoft HR Payroll	5.0	2.0	2.0	4.0	3.0	8.0	2.0	3.0	4.0	33.0
WIN Server - W2K3APPS13PT	PeopleSoft HR Payroll	5.0	2.0	2.0	4.0	3.0	8.0	2.0	3.0	4.0	33.0
WIN Server - W2K3APPS15	County Attorney Applications	4.0	2.0	7.0	3.0	2.0	8.0	2.0	3.0	1.0	32.0
WIN Server - W2KAPPS05	Revenue Commission (CARS)	3.0	2.0	7.0	2.0	2.0	6.0	2.0	2.0	1.0	27.0
PERIMETER AUDITS											
Firewall(s)	Perimeter Firewalls	4.0	2.0	7.0	3.0	3.0	6.0	3.0	3.0	1.0	32.0
Penetration Testing	External & Internal Penetration Testing	4.0	-	7.0	2.0	2.0	6.0	3.0	1.0	-	25.0
(All External & Internal Web Servers)											
OTHER STANDARD TECHNOLOGY AUDITS											
Active Directory	Network Authentication	3.0	3.0	7.0	3.0	-	4.0	3.0	3.0	2.0	28.0
Change Control Management	Departmental Change Control Policy	3.0	3.0	7.0	3.0	-	4.0	1.0	3.0	1.0	25.0
Data Center Controls	Datacenter Security & Environmental	3.0	3.0	7.0	2.0	2.0	4.0	3.0	2.0	1.0	27.0
Disaster Recovery	DR Business Continuity Plan	4.0	3.0	2.0	4.0	3.0	8.0	-	3.0	2.0	29.0
Email Usage & Control	Email Usage, Archival, and Legal	4.0	3.0	7.0	4.0	2.0	6.0	2.0	3.0	2.0	33.0
Software Compliance	Software Audit	2.0	3.0	7.0	3.0	-	6.0	2.0	2.0	1.0	26.0
System Development	Application Development Controls	4.0	3.0	7.0	3.0	2.0	4.0	2.0	3.0	2.0	30.0



Risk Factor ASSIGNMENT

Company Name

AUDIT TECHNOLOGIES	DESCRIPTION	Level of Government Reliance	Commercial vs. Internal	Last Audit	Internal Customer Impact	External Customer Impact	Potential Financial Exposure	Security Threat	Level of Admin Tasks	Major Recent Changes
APPLICATIONS SECURITY & CONTROL AUDITS										
Oracle Financials	Financial Management	XX High	Commercial	Last Year	XX High	XX High	XX High	Medium	Medium	Medium
PeopleSoft HR Payroll	Human Resource Management	XX High	Commercial	Last Year	XX High	Medium	XX High	Medium	High	High
Risk Management	Worker's Comp. & Child Support	High	Internal	None	Medium	Medium	Medium	Medium	Low	None
Chevin Fleet Management	Government Fleet Management	Medium	Commercial	None	Medium	Low	Medium	Low	Low	High
Cashier	Payment Processing to Oracle	Medium	Internal	None	Medium	Low	Medium	Low	Low	None
AIM	EMS Billing Application	High	Internal	None	Medium	High	High	Low	Low	Low
IMS	Inmate Management System	XX High	Commercial	None	High	Low	Low	Medium	Low	None
DATABASE SECURITY & CONTROL AUDITS										
Oracle DB	Oracle Financials Database	XX High	Commercial	Last Year	High	Medium	High	Low	Medium	None
SQL Server 2000 - W2K3DB05	PeopleSoft HR Payroll Database	High	Commercial	Last Year	High	Medium	High	Low	Medium	Medium
SQL Server 2000 - W2K3DB02	Risk Management Database	XX High	Commercial	None	High	Low	Medium	Low	Low	None
SQL Server 2000 - W2K3DB01	Fleet Management Cashier Database	Medium	Commercial	None	Medium	N/A	Low	Low	Low	High
SQL Server 2000 - W2K3DBDEV02	Authorization Manager Database	Medium	Internal	None	Medium	None	None	Medium	Medium	Medium
PLATFORMS/SERVER AUDITS										
AIX Server - Oracle Financials	Oracle Financials	XX High	Commercial	Last Year	High	High	High	Low	Medium	Medium
WIN Server - W2K3APPS14PT	PeopleSoft HR Payroll	XX High	Commercial	Last Year	High	Medium	High	Low	Medium	High
WIN Server - W2K3APPS13PT	PeopleSoft HR Payroll	XX High	Commercial	Last Year	High	Medium	High	Low	Medium	High
WIN Server - W2K3APPS15	County Attorney Applications	High	Commercial	None	Medium	Low	High	Low	Medium	None
WIN Server - W2KAPPS05	Revenue Commission (CARS)	Medium	Commercial	None	Low	Low	Medium	Low	Low	None
PERIMETER AUDITS										
Firewall(s)	Perimeter Firewalls	High	Commercial	None	Medium	Medium	Medium	Medium	Medium	None
Penetration Testing	External & Internal Penetration Testing	High	N/A	None	Low	Low	Medium	Medium	None	N/A
(All External & Internal Web Servers)										
OTHER STANDARD TECHNOLOGY AUDITS										
Active Directory	Network Authentication	Medium	Internal	None	Medium	N/A	Low	Medium	Medium	Low
Change Control Management	Departmental Change Control Policy	Medium	Internal	None	Medium	N/A	Low	None	Medium	None
Data Center Controls	Datacenter Security & Environmental	Medium	Internal	None	Low	Low	Low	Medium	Low	None
Disaster Recovery	DR Business Continuity Plan	High	Internal	Last Year	High	Medium	High	N/A	Medium	Low
Email Usage & Control	Email Usage, Archival, and Legal	High	Internal	None	High	Low	Medium	Low	Medium	Low
Software Compliance	Software Audit	Low	Internal	None	Medium	N/A	Medium	Low	Low	None
System Development	Application Development Controls	High	Internal	None	Medium	Low	Low	Low	Medium	Low



Risk Factor DEFINITIONS

Company Name

Corporate Reliance	
Rating	Factor
XX High	5.0
High	4.0
Medium	3.0
Low	2.0
None	1.0
N/A	0.0

Commercial vs. Internally Developed	
Rating	Factor
Internal	3.0
Commercial	2.0
None	1.0
N/A	0.0

Prior Audit	
Period	Factor
Current Year	1.0
Last Year	2.0
2 Yrs Prior	3.0
3 Yrs Prior	4.0
4 Yrs Prior	5.0
5 Yrs Prior	6.0
None	7.0
N/A	0.0

Internal Customer Impact	
Rating	Factor
XX High	5.0
High	4.0
Medium	3.0
Low	2.0
None	1.0
N/A	0.0

External Customer Impact	
Rating	Factor
XX High	5.0
High	4.0
Medium	3.0
Low	2.0
None	1.0
N/A	0.0

Financial Exposure	
Rating	Factor
XX High	10.0
High	8.0
Medium	6.0
Low	4.0
None	2.0
N/A	0.0

Security Threat	
Rating	Factor
XX High	5.0
High	4.0
Medium	3.0
Low	2.0
None	1.0
N/A	0.0

Level of Admin Tasks	
Rating	Factor
High	4.0
Medium	3.0
Low	2.0
None	1.0
N/A	0.0

Recent Major Change	
Rating	Factor
High	4.0
Medium	3.0
Low	2.0
None	1.0
N/A	0.0



Information Technology Matrix Frequently Asked Questions

How often should the Matrix be updated?

The Matrix should be updated on an annual basis. Acquired technologies should be included and each risk factor should be re-assessed.

How do I update the Matrix?

To update the Matrix add or modify the technology items in worksheet '1.1 - Risk Matrix'. Place the added or modified technology item under the appropriate category (see column 'A'); then assign the risk-levels for the corresponding factors. This will automatically update worksheet '1.0 - Risk Matrix'. Review the 'Summary' worksheet to ensure the risk score updated properly. Now sort the data based upon your needs.

For security purposes certain worksheets and worksheet fields have been protected. You will need to obtain the password to access these fields to update the Matrix.

Can I add new technologies to the Matrix?

Yes.

Can I add additional factors?

To add additional factors please contact Securance Consulting. We recognize the diversity in our clients and will add customization based on client requests.

Can I change the factor values?

Yes. Factor values can be changed to values that are currently used by your organization.

For security purposes certain worksheets and worksheet fields have been protected. You will need to obtain the password to access these fields to update the Matrix.



Information Technology Matrix Frequently Asked Questions

How are each year's projects determined?

After updating the Matrix the Summary report should be reviewed and the technologies with the highest score become candidates for current year audits.

How can I have the Matrix customized?

Please contact Securance Consulting for further customization of the Technology Risk Matrix.

Can we incorporate operational and financial risks?

Yes. The Technology Risk Matrix is designed to allow for maximum flexibility and customization. It can be incorporated into other existing risk models or be expanded to incorporate operational and financial risk.

