

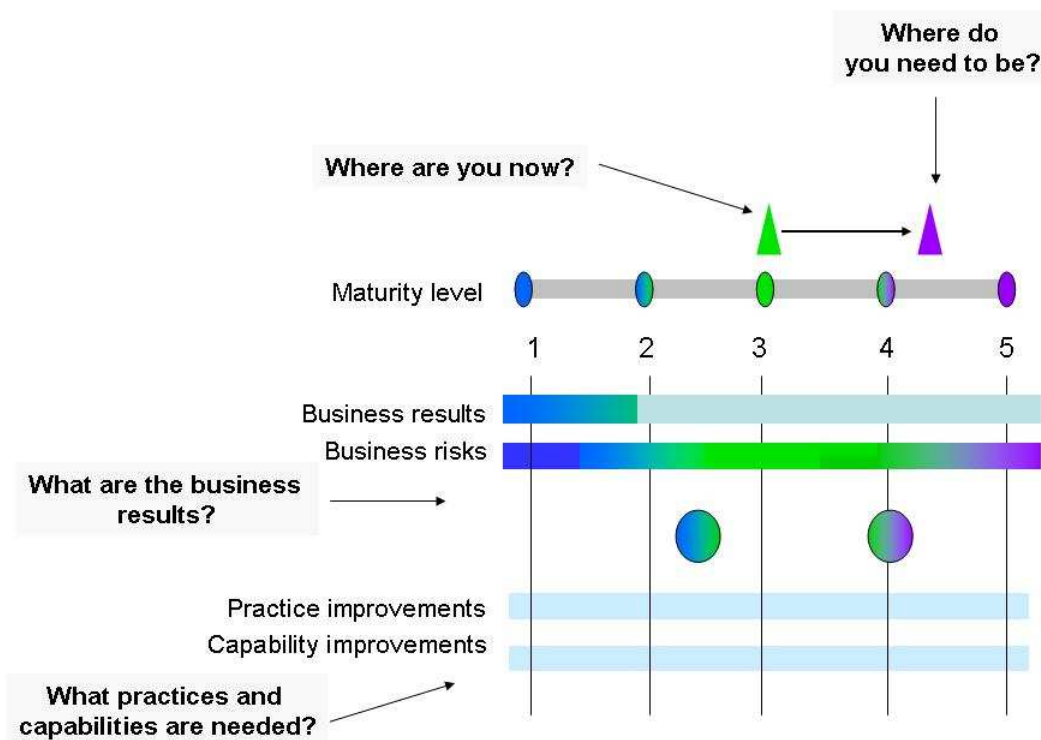
Guide to the Interactive Tools

The interactive tools on the IT PCG Site provide a quick way to benchmark the maturity of the organization against more than 2,600 organizations from around the World, assess what the business outcomes are relative to others, and how to improve these outcomes.

Assess, improve, measure

Improving IT GRC maturity practices is its own quality improvement procedure that, at its core, simply means assessing the current state of IT GRC maturity, identifying which maturity profile is optimum for the organization based on business and financial results, identifying gaps in current practices, improving practices and capabilities, and measuring the results (see Figure 1).

Figure 1. Assess, improve, measure



Source: IT Policy Compliance Group, 2008

Some practices and capabilities in the firm may be further ahead than what is required to improve results, while other practices and capabilities will be further behind. After improving capabilities and practices, it is always of good idea to measure results to determine if objectives have been met or not, and to identify the next steps to take.

Three Examples: Britain, Singapore and the US

This Guide to Leveraging the Interactive Tools for IT GRC employs three example companies to illustrate three different examples of how to interpret and use the results

from the Interactive Tools. Although the organizations are fictitious, the IT GRC maturity, business outcomes, spending on regulatory compliance and financial risk cited are not: these are from the benchmarks conducted with more than 2,600 organizations from around the World. The examples include:

- (1) A company located in Britain in the medical device and pharmaceutical industries with annual revenues of £ 2,100,000,000 British Pounds
- (2) A firm located in Singapore in the electronic manufacturing industry with annual revenues of \$1,000,000,000 Singapore Dollars
- (3) An organization located in the United States in the banking and financial services industry with annual revenues of \$1,000,000,000 US Dollars

Example, British Medical Device and Pharmaceutical Company

Find existing IT GRC maturity score

This company uses the interactive tool to find its IT GRC maturity. The inputs for the tool include:

- Balanced Scorecard = Yes
- Quality Improvement Program = Yes
- CIS benchmarks = Yes
- Percentage of technical controls = 50 percent
- Frequency of assessment = 12 times per year

Current maturity score is 3.71

The output from the rapid assessment is as follows:

- **IT GRC Maturity Score = 3.71**

Determine operating results at existing maturity level

At a maturity level of 3.71, the business outcomes for this firm are, as follows

- Customer service = 2.9 percent above industry norm
- Customer retention = 2.3 percent above norm
- Revenue = 2.9 percent above norm
- Profits = 2.5 percent above norm

Change in operating results at target maturity level 4.5

This firm decides it would like to improve its IT GRC maturity to 4.5, from its current level of 3.71. When moving the maturity slider to 4.5 on the business results tool, the organization finds that its business metrics will improve, as follows:

- Customer service = 6.6 percent above norm
- Customer retention = 5.1 percent above norm
- Revenue = 6.4 percent above norm
- Profits = 5.2 percent above norm

Results at target maturity of 4.5

Improvements to IT GRC maturity should result in revenue that is £2,173,500,000, a £73,500,000 increase after the improvements have been completed. Operating with a 10

percent profit margin prior to the improvements, profits should increase to £223,218,450 after the improvements, from £210,000,000 before the improvements. This is a net increase in profit of £13,218,450 (Table 1).

Table 1: Change in Operating Results

	Before	After	Net change
Revenue	£2,100,000,000	£2,173,500,000	£73,500,000 increase
Profits	£210,000,000	£223,218,450	£13,218,450 increase
Customer satisfaction	2.9% above norm	6.6% above norm	3.7% increase
Customer retention	2.3% above norm	5.1% above norm	2.8% increase

Source: IT Policy Compliance Group, 2008

If this organization wants to increase operating results further, it would increase the target maturity level higher than 4.5.

Change in financial loss and risk from the loss or theft of customer data

Operating at a maturity level of 3.71, this company is likely to lose £77.3 million once every 8 years. This is equivalent to a loss that is roughly £5.8 million annually. As a result of selecting a target level of 4.5 for IT GRC maturity, the firm should expect this financial risk to be reduced to £37.8 million once every 47 years, an equivalent loss that is roughly £804,700 annually (Table 2).

Table 2: Change in Financial Loss and Risk

	Before	After	Net change
Loss when event occurs	£77.3 million	£37.8 million	£39.5 million decrease
Frequency of occurrence	Once every 8 years	Once every 47 years	39 year increase
Annualized loss	£5.8 million per year	£804,700 per year	£5 million per year lower

Source: IT Policy Compliance Group, 2008

If this organization wants to reduce financial risk further, then the target maturity rate would be established higher than the selected 4.5 level.

Change in spend on regulatory compliance

At its current revenue and a maturity of 3.7, this firm is spending, on average, £12.8 million annually on regulatory compliance. This rate of spend represents a 14 percent savings from the industry maximum, which is £14.8 million per year (Table 3).

Table 3: Change in Spend on Regulatory Compliance

	Before	After	Net change
Annual spend	£12.8 million	£9.6 million	£3.2 million decrease

Source: IT Policy Compliance Group, 2008

Improving its IT GRC maturity to 4.5 should result in a decline in spending on regulatory compliance, to £9.6 million annually, a 35 percent savings from the maximum and a 25 percent decline from its current rate of spend. The savings from improvements made to IT GRC maturity, on regulatory spend amount to £3.2 million annually.

Practices and capabilities to improve results

The company is currently operating at maturity level 3.71 and desires to achieve operating results, financial loss and risk, and spend on regulatory compliance at a new maturity level of 4.5. Achieving this will require changes to existing practices for IT GRC accompanied by capabilities to implement the practices.

When consulting the practices and capability tables of the IT GRC CMM, the company should identify the practices and capabilities of levels 2, 3, 4 and 5 to determine:

- Which of its existing practices are already between levels 4 and 5
- Which of its existing practices are already below level 3
- Changes in practices that will require longer-term, phased projects
- Changes to practices that can be achieved with short-term projects

Managing the IT portfolio

By increasing the maturity of its IT GRC practices, the company will experience an increase in profits, decreases in spend on regulatory compliance, increases in customer satisfaction and retention, while mitigating financial risk from the loss of customer data. When evaluating the financial contribution from improvements to IT GRC, it will be important to separate one-time charges from recurring annual expenses that may be eliminated or those being added. It is also important to evaluate the relative contribution of IT GRC maturity improvements to customer satisfaction and customer retention when compared with other portfolio projects that may have direct impacts on top- and bottom-line results for the organization (Table 4).

Table 4: Financial Return

Source	Net change	Percentage of total
Annual profit	£13,218,450 higher	62%
Annual spend on regulatory compliance	£3,200,000 lower	15%
Annual loss avoided – customer data loss/theft	£5,000,000 lower	23%
Annual contribution	£21,418,450	100%

Source: IT Policy Compliance Group, 2008

Example, Singapore Electronic Manufacturing Company

Find existing IT GRC maturity score

This company uses the interactive tool to find its IT GRC maturity. The inputs for the tool include:

- Balanced Scorecard = No
- Quality Improvement Program = Yes
- CIS benchmarks = No
- Percentage of technical controls = 52 percent
- Frequency of assessment = 18 times per year

Current maturity score is 3.01

The output from the rapid assessment is as follows:

- **IT GRC Maturity Score = 3.01**

Determine current operating results at existing maturity level

At a maturity level of 3.01, the current business outcomes for this firm are, as follows

- Customer service = 0 percent (at industry norm)
- Customer retention = 0 percent (at industry norm)
- Revenue = 0 percent (at industry norm)
- Profits = 0 percent (at industry norm)

Change in operating results at target maturity level 4.5

The firm decides it would like to improve its IT GRC maturity to 4.5, from its current level of 3.01. When moving to the maturity slider to 4.5 on the business results tool, the organization finds that its business metrics will improve, as follows:

- Customer service = 6.6 percent above norm
- Customer retention = 5.1 percent above norm
- Revenue = 6.4 percent above norm
- Profits = 5.2 percent above norm

Results at target maturity of 4.5

Improvements to IT GRC maturity should result in revenue that is \$1,064,000,000, a \$64,000,000 increase after the improvements have been completed. Operating with a 10 percent profit margin prior to the improvements, profits should increase to \$111,932,800 after the improvements, from \$100,000,000 before the improvements. This is a net increase in profit of \$11,932,800 (Table 5).

Table 5: Change in Operating Results

	Before	After	Net change
Revenue	\$1,000,000,000	\$1,064,000,000	\$64,000,000
Profits	\$100,000,000	\$111,932,800	\$11,932,800 increase
Customer satisfaction	0 % at industry norm	6.6% above norm	6.6% increase
Customer retention	0% at industry norm	5.1% above norm	5.1% increase

Source: IT Policy Compliance Group, 2008

If this organization wants to increase operating results further, it would target a maturity level that is higher than 4.5.

Change in financial loss and risk from the loss or theft of customer data

Operating at a maturity level of 3.01, this company is likely to lose \$48 million once every 8.6 years. This is equivalent to a loss that is roughly \$5.6 million annually. As a result of selecting a target level of 4.5 for IT GRC maturity, the firm should expect this financial risk to be reduced to \$18 million once every 46.3 years, an equivalent loss that is roughly \$389,000 annually (Table 6).

Table 6: Change in Financial Loss and Risk

	Before	After	Net change
Loss when event occurs	\$48 million	\$18 million	\$30 million decrease
Frequency of occurrence	Once every 8.6 years	Once every 46.3 years	37.7 year increase
Annualized loss	\$5.6 million per year	\$389,000 per year	\$5.2 million per year lower

Source: IT Policy Compliance Group, 2008

If this organization wants to reduce financial risk further, then the target maturity rate would be established higher than the selected 4.5 level.

Change in spend on regulatory compliance

At its current revenue and a maturity of 3.01, this firm is spending, on average, \$5.4 million annually on regulatory compliance. This rate of spend represents a 3 percent savings from the industry maximum, which is \$5.5 million per year (Table 7).

Table 7: Change in Spend on Regulatory Compliance

	Before	After	Net change
Annual spend	\$5.4 million	\$3.6 million	\$1.78 million decrease

Source: IT Policy Compliance Group, 2008

Improving its IT GRC maturity to 4.5 should result in a decline in spending on regulatory compliance to \$3.6 million annually, a 35 percent savings from the maximum and a 33

percent decline from its current rate of spend. The savings from improvements made to IT GRC maturity, on regulatory spend amounts to \$1.78 million annually.

Practices and capabilities to improve results

This company is currently operating at maturity level 3.01 and desires to achieve operating results, financial loss and risk, and spend on regulatory compliance at a new maturity level of 4.5. Achieving this will require changes to existing practices for IT GRC accompanied by capabilities to implement the practices.

When consulting the practices and capability tables of the IT GRC CMM, the company will want to identify the practices and capabilities of levels 2, 3, 4 and 5 to determine:

- Which of its existing practices are already between levels 4 and 5
- Which of its existing practices are already below level 3
- Changes in practices that will require longer-term, phased projects
- Changes to practices that can be achieved with short-term projects

Managing the IT portfolio

By increasing the maturity of its IT GRC practices, the company will experience an increase in profits, decreases in spend on regulatory compliance, increases in customer satisfaction and retention, while mitigating financial risk from the loss of customer data. When evaluating the financial contribution from improvements to IT GRC, it will be important to separate one-time charges from recurring annual expenses that may be eliminated or those being added. It is also important to evaluate the relative contribution of IT GRC maturity improvements to customer satisfaction and customer retention when compared with other portfolio projects that may have direct impacts on top- and bottom-line results for the organization (Table 8).

Table 8: Financial Return

Source	Net change	Percentage of total
Annual profit	\$11,932,800 higher	63%
Annual spend on regulatory compliance	\$1,780,000 lower	9%
Annual loss avoided – customer data loss/theft	\$5,200,000 lower	28%
Annual contribution	\$18,912,800	100%

Source: IT Policy Compliance Group, 2008

Example, United States Banking and Financial Services Firm

Find existing IT GRC maturity score

This company uses the interactive tool to find its IT GRC maturity. The inputs for the tool include:

- Balanced Scorecard = Yes
- Quality Improvement Program = No
- CIS benchmarks = Yes
- Percentage of technical controls = 42 percent
- Frequency of assessment = 6 times per year

Current maturity score is 2.51

The output from the rapid assessment is as follows:

- **IT GRC Maturity Score = 2.51**

Determine operating results at existing maturity level

At a maturity level of 2.51, the business outcomes for this firm are, as follows

- Customer service = 2.0 percent below industry norm
- Customer retention = 1.7 percent below norm
- Revenue = 2.0 percent below norm
- Profits = 1.8 percent below norm

Change in operating results at target maturity level 4.5

The firm decides it would like to improve its IT GRC maturity to 4.5, from its current level of 2.51. When moving the maturity slider to 4.5 on the business results tool, the organization finds that its business metrics will improve, as follows:

- Customer service = 6.6 percent above norm
- Customer retention = 5.1 percent above norm
- Revenue = 6.4 percent above norm
- Profits = 5.2 percent above norm

Results at target maturity of 4.5
--

Improvements to IT GRC maturity should result in revenue that is \$1,086,000,000, an \$86,000,000 increase after the improvements have been completed. Operating with a 10 percent profit margin prior to the improvements, profits should increase to \$117,722,400 after the improvements, from \$100,000,000 before the improvements. This is a net increase in profit of \$17,722,400 (Table 9).

Table 9: Change in Operating Results

	Before	After	Net change
Revenue	\$1,000,000,000	\$1,086,000,000	\$86,000,000 increase
Profits	\$100,000,000	\$117,722,400	\$17,772,400 increase
Customer satisfaction	2.0% below norm	6.6% above norm	8.6% increase
Customer retention	1.7% below norm	5.1% above norm	6.8% increase

Source: IT Policy Compliance Group, 2008

If the organization wants to increase operating results further, it would increase the target maturity level higher than 4.5.

Change in financial loss and risk from the loss or theft of customer data

Operating at a maturity level of 2.51, this company is likely to lose \$56 million once every 7 years. This is equivalent to a loss that is roughly \$8.1 million annually. As a result of selecting a target level of 4.5 for IT GRC maturity, the firm should expect this financial risk to be reduced to \$18 million once every 47 years, an equivalent loss that is roughly \$382,000 annually (Table 10).

Table 10: Change in Financial Loss and Risk

	Before	After	Net change
Loss when event occurs	\$56 million	\$18 million	£39.5 million decrease
Frequency of occurrence	Once every 7 years	Once every 47 years	40 year increase
Annualized loss	\$8.1 million per year	\$382,000 per year	\$7.7 million per year lower

Source: IT Policy Compliance Group, 2008

If the organization wants to reduce financial risk further, then the target maturity rate would be established higher than the selected 4.5 level.

Change in spend on regulatory compliance

At its current revenue and a maturity of 2.51, this firm is spending, on average, \$7.6 million annually on regulatory compliance. This rate of spend is at the industry norm, at \$7.6 million per year (Table 11).

Table 11. Change in Spend on Regulatory Compliance

	Before	After	Net change
Annual spend	\$7.6 million	\$4.9 million	\$3 million decrease

Source: IT Policy Compliance Group, 2008

Improving its IT GRC maturity to 4.5 should result in a decline in spending on regulatory compliance, to \$4.9 million annually, a 35 percent savings from its current rate of spend.

The savings from improvements made to IT GRC maturity, on regulatory spend amounts to \$3 million annually.

Practices and capabilities to improve results

The company is currently operating at maturity level 2.51 and desires to achieve operating results, financial loss and risk, and spend on regulatory compliance at a new maturity level of 4.5. Achieving this will require changes to existing practices for IT GRC accompanied by capabilities to implement the practices.

When consulting the practices and capability tables of the IT GRC CMM, the company will want to identify the practices and capabilities of levels 2, 3, 4 and 5 to determine:

- Which of its existing practices are already between levels 4 and 5
- Which of its existing practices are already below level 2
- Changes in practices that will require longer-term, phased projects
- Changes to practices that can be achieved with short-term projects

Managing the IT portfolio

By increasing the maturity of its IT GRC practices, the company will experience an increase in profits, decreases in spend on regulatory compliance, increases in customer satisfaction and retention, while mitigating financial risk from the loss of customer data.

When evaluating the financial contribution from improvements to IT GRC, it will be important to separate one-time charges from recurring annual expenses that may be eliminated or those being added. It is also important to evaluate the relative contribution of IT GRC maturity improvements to customer satisfaction and customer retention when compared with other portfolio projects that may have direct impacts on top- and bottom-line results for the organization (Table 12).

Table 12, Financial Return

Source	Net change	Percentage of total
Annual profit	\$17,722,400 higher	62%
Annual spend on regulatory compliance	\$3,000,000 lower	11%
Annual loss avoided – customer data loss/theft	\$7,700,000 lower	27%
Annual contribution	\$28,422,400	100%

Source: IT Policy Compliance Group, 2008

Maturity, Results, Practices and Capabilities

IT GRC maturity is all about the intersection of people, business procedures and the use of technology to achieve business objectives. As such, some practices and capabilities are more important than others in being able to improve operating results, reduce financial risk, and lower expenses. The benchmarks show that emphasizing one practice or capability, to the exclusion of others, will not result in material improvement to maturity and business outcomes. However, the benchmarks also show that some practices and capabilities influence results more markedly than others (Table 13).

Table 13, ITS Maturity, Practices and Capabilities

IT GRC Maturity	Balanced Scorecard	Continuous quality improvement	CIS benchmarks	Percentage of technical controls	Frequency of data controls assessment per year
0	Yes	Yes	Yes	0	1
2.5	No	Yes	No	50%	9
3.0	Yes	Yes	Yes	30%	9
3.5	No	No	No	100%	100
4.0	Yes	Yes	Yes	50%	18
4.5	Yes	Yes	Yes	67%	27

Source: IT Policy Compliance Group, 2008

As Table 12 shows, focusing only on continuous measurement, in a highly automated environment involving 100% technical controls (example: production telecommunication deployments), the maximum that can be achieved is a maturity of 3.5.

The least mature example, shown at a maturity of 0, is where the management systems for a balanced scorecard, a continuous quality improvement program and the use of the CIS benchmarks in IT are accompanied by no technical controls and monitoring and reporting that are occurring only once per year.

The most mature example, illustrated with a maturity of 4.5, is where the management systems, including the use of a balanced scorecard, a continuous quality improvement program and the CIS benchmarks in IT, are accompanied by two-thirds technical controls and measurement, monitoring and reporting occurring 27 times per year.

CRC CMM Tables

The capabilities and practices of the empirical IT GRC Capability Maturity Model (GRC CMM) are mapped from 1 to 5, from least mature to most mature (Table 14). The capabilities and practices within the GRC CMM currently consist of the following:

- Organizational competencies and practices;
- Capabilities within IT
- Culture, budgeting and spending
- Third-party IT services, outsourcing and off-shoring
- Continuous quality improvement

- Behavior and use of frameworks by senior managers and in IT
- Employee training and education
- Spending on IT assurance, IT security and IT audit
- Actions that improve results
- Policies, objectives and controls
- Continuous measurement, monitoring and reporting
- Change management in and prevention in IT.

The practices and capabilities of the GRC CMM are displayed by maturity level, corresponding to the business outcomes that are documented by the research conducted with more than 2,600 organizations around the World. This empirical approach provides the ability to identify the practices and capabilities that will improve results.

Depending on the IT GRC maturity scores, it is recommended that practices and capabilities at a level below the current maturity level be consulted. Similarly, it is recommended that practices and capabilities at a level below, and above if applicable, the target maturity level be consulted.

This bracketing of practices and capabilities, from current to target levels, enables an assessment of current practice against industry averages at each level of maturity and business outcome, and provides greater insight into whether the organization is ahead of what is required, or behind.

Identifying the gaps, at current and target maturity levels, will allow organizations to identify where the least, and most improvements to practices and capabilities are needed.

Notes about Practices and Capabilities

Capabilities are the capacity on hand within an organization to take action, or the ability to implement a practice, that will improve IT GRC results and business outcomes.

Example: employee education and training

As an example of this, consistent on-demand employee education and training is widely shown to improve results. And, while on-demand may be the most common way to implement this practice, some organizations have opted to augment employee education and training with carrots and sticks when it comes to protecting customer data by penalizing employee compensation plans when customer data is lost or stolen, and rewarding employees for finding problems in inadequate procedural and technical controls that are employed to protect customer data.

Example: Frequency of monitoring, measurement and reporting

Similarly, consistent controls monitoring, measurement and reporting, taking place weekly for protecting customer data, are shown to improve results. However, to achieve this, the most mature organizations are automating the prevention of unauthorized change while automating the controls and activities related to protecting information in the custody of IT systems, applications and networks: measuring and reporting on effectiveness of controls weekly. The capability for very frequent monitoring, measurement, reporting and prevention is shown to be technologies among the most mature organizations.

Table 14, GRC CMM maturity spectrum

IT GRC maturity level	Description
Level 0	<p>Nonexistent procedures and practices</p> <p>There is no ongoing oversight of IT related activities to ensure that an enterprise's IT services add value to the organization and that IT-related risks are appropriately managed.</p>
Level 1	<p>Initial/ad hoc procedures and practices</p> <p>IT initiatives are driven by senior managers and primary business stakeholders, based on the changing needs of the business. Problems are resolved on a project basis with teams formed and dissolved as needed. Routine governance activities do <i>not</i> take place. No one realizes that more formalized oversight of IT is required.</p>
Level 2	<p>Repeatable but intuitive procedures and practices</p> <p>Governance of IT depends on the experience of IT managers, with limited involvement from business stakeholders. Most IT initiatives are funded based on prior year spending, with little flexibility built in for expected business change. Senior managers become involved in IT when major business initiatives are off-track. IT successes or failures are typically limited to technical measures. Oversight of IT is focused on case-by-case business issues that arise.</p>
Level 3	<p>Defined procedures and practices</p> <p>Informal practices are formalized and institutionalized, with relatively simple and unsophisticated measurement and assessment techniques. Specific procedures are developed to govern IT activities. External audit frameworks are utilized to assess the effectiveness of IT in delivering value. The mitigation of risk from IT operations is handled on a case-by-case basis with no consistency.</p>
Level 4	<p>Managed and measured procedures and practices</p> <p>Procedural and practice frameworks are defined for oversight and management of IT activities. These frameworks are used as the basis for governance of IT in the organization. Common IT procedures are identified and selected areas for improvement are based on these. Senior management team reviews value delivery and risks related to IT. Spending on IT is based on a mixture of value and risk metrics.</p>
Level 5	<p>Optimized and balanced procedures and practices</p> <p>Senior management has enough information about IT to make informed business decisions without being personally involved in "running IT." IT activities are optimally directed to deliver business value and avoid business risk, both of which are measured, with backup plans to correct deviations and problems. Continuous Quality Improvement programs are implemented to consistently measure deviations from objectives. Continuous improvement of prioritized IT capabilities is embedded and benchmarked against internal and external metrics, as well as internal and external audit results. Spending on IT is optimized and changed to deliver the greatest value at a risk appropriate for the organization.</p>

Source: IT Policy Compliance Group, 2008