


## IT GRC CMM Capabilities and Practices

Primary benchmark research conducted by the IT Policy Compliance Group during the past two years has resulted in an empirical IT Governance Risk and Compliance Capability Maturity Model (GRC CMM) with specific practices, competencies, and capabilities that are directly related to business and financial outcomes of organizations at each maturity level.

This fact-based GRC Capability Maturity Model can be used to assess current maturity levels and quantify the business outcomes associated with each maturity level, as well as identify desired business outcomes and the capabilities, practices, and competencies needed to improve results.

The IT GRC CMM maps business outcomes from worst to the best, from the lowest level (1) to the highest level (5) on the IT GRC maturity scale.

**Figure 1. IT GRC maturity capability model**

N: 2,608      Least mature  Most mature

IT GRC maturity level	1	2	3	4	5
Population	20%	68%			12%
Non existent practices and procedures	Initial - ad hoc procedures and practices	Repeatable but intuitive procedures and practices	Defined procedures and practices	Managed and measured procedures and practices	Optimized and balanced procedures and practices
Business result metrics	Lowest results	Lowest to highest results			Highest results
Financial impact from data loss or theft and IT service level disruptions	Highest financial risk	Highest to lowest			Lowest financial risk
IT GRC business risk indicators	Highest	Highest to lowest			Lowest

Source: IT Policy Compliance Group, 2008

The descriptions of the maturity levels for GRC in this report are similar to and borrow from much previous research, including significant contributions and support of the supporting members of the IT Policy Compliance Group, including the Computer Security Institute, ISACA (the Information Systems Audit and Control Association) the IIA (the Institute of Internal Auditors), the IT Governance Institute, Protiviti, and Symantec.

However, after the scale and descriptions of the maturity levels, the empirical GRC CMM differs from other maturity models in three principal ways, as follows:

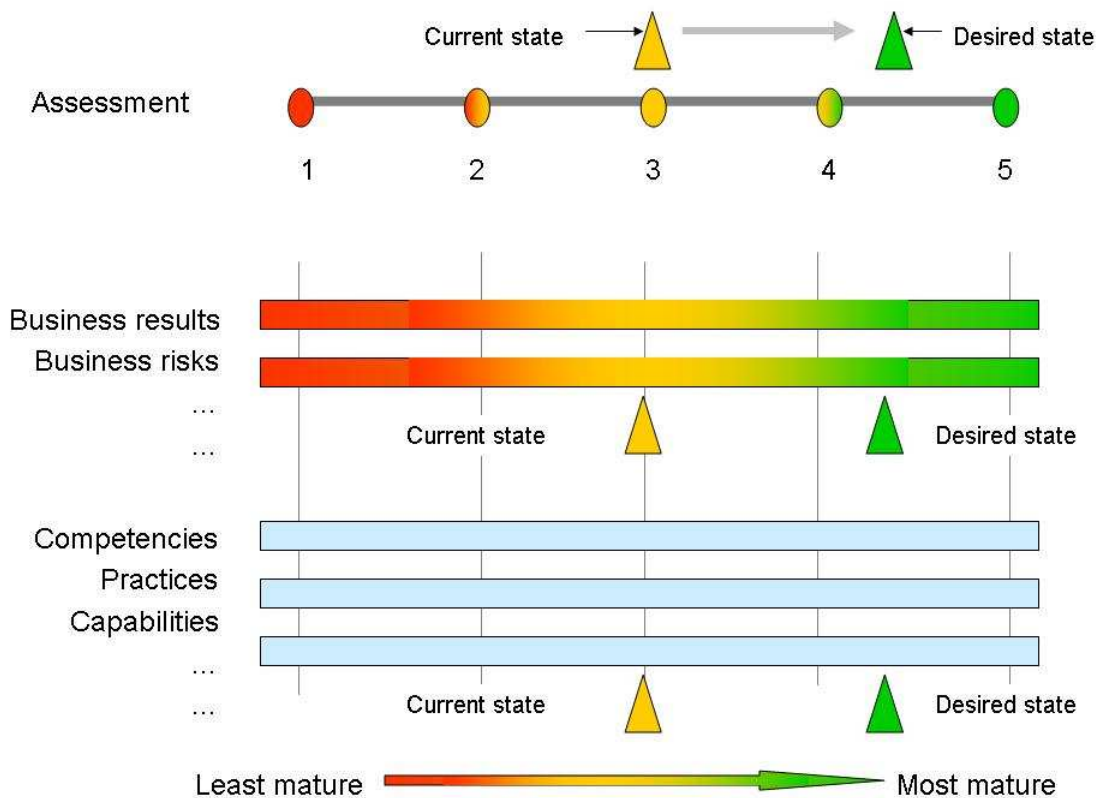
- 1) The findings are focused exclusively on IT GRC.
- 2) The maturity described by the report is directly linked to business outcomes and financial losses
- 3) The practices and capabilities are directly related to the business outcomes and financial losses.

If a result, a practice or a capability is not grounded in the reality of actual experience, it is not contained in the GRC CMM. The competencies, capabilities, and practices associated with each maturity level in the GRC CMM are those of the firms with specific business results at each level. This basis for the practices, capabilities, and competencies in the GRC CCM delivers empirical insight into what is working and not working, based upon facts, not hypothesis.

### Improving competencies, practices, and capabilities

The capabilities, practices, and competencies directly associated with higher GRC CCM maturity levels provide the opportunity to diagnose specific shortfalls or misaligned activities that a firm may already have implemented (see Figure 3).

**Figure 2. Managing improvements to IT GRC maturity**



Source: IT Policy Compliance Group, 2008

For instance, an organization may have implemented continuous monitoring but may find that its Continuous Quality Improvement program is based on vague or nonexistent metrics that stifle its progress. Or, a firm may find that it has implemented a balanced scorecard for the alignment of value delivered by IT without any of the underlying practices necessary to enhance IT GRC maturity.

Some organizations may find that moving from their current state of maturity will require an incremental approach through planned stages. In this case, it is critical to identify the shortfalls against benchmarked practices and capabilities and develop phased plans that are based on priorities to improve specific practices as part of a longer-term plan for improving results.

Making improvements to business outcomes and GRC practices can be accomplished with the assistance of these IT GRC CMM Tables. In addition, interactive assessment tools at the IT Policy Compliance Group website ([www.itpolicycompliance.com](http://www.itpolicycompliance.com)) will provide an automated method to assess the current maturity of the organization, the business outcomes for each level of maturity, and the improvements that can be targeted.

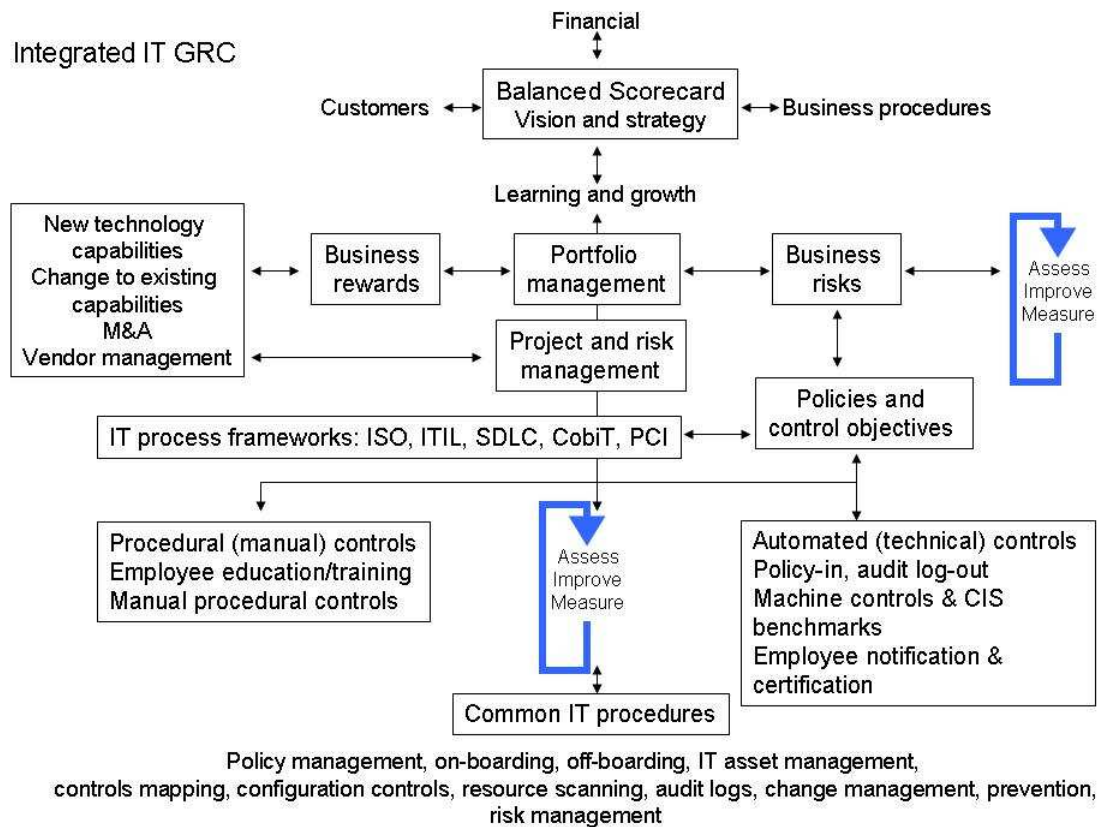
## IT GRC CMM Capability and Practice Tables

Table 1. GRC CMM maturity spectrum

IT GRC maturity level	Description
Level 0	<p><b>Nonexistent procedures and practices</b></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><b>Initial/ad hoc procedures and practices</b></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><b>Repeatable but intuitive procedures and practices</b></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><b>Defined procedures and practices</b></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><b>Managed and measured procedures and practices</b></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><b>Optimized and balanced procedures and practices</b></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

**Figure 3. Organizational competency: Integrated IT GRC**



Source: IT Policy Compliance Group, 2008

**Table 2. Organizational competencies among the most mature**

<ul style="list-style-type: none"> <li>• Senior management involvement</li> <li>• Audit committee involvement</li> <li>• IT, legal, internal audit, and finance leadership</li> <li>• Employee training and a culture of compliance</li> <li>• Improvements to IT risk assessments, data protection, IT audit, risk, and compliance practices and capabilities</li> <li>• Adjustments to spending in IT to support needed capabilities</li> <li>• A Continuous Quality Improvement program for IT GRC</li> <li>• An integrated IT GRC program</li> </ul>
--

Source: IT Policy Compliance Group, 2008

**Table 3. Practices and capabilities among the most mature**

<ul style="list-style-type: none"> <li>• Access to sensitive and protected data on PCs and laptops is segmented and protected.</li> <li>• Meaningful and measurable control objectives and policies are employed, based on business risks.</li> <li>• IT policies, process frameworks, and control objectives are mapped to one another.</li> <li>• Common IT procedures are employed for audit.</li> <li>• Three times more controls than objectives are employed.</li> <li>• Consistent configurations and common IT procedures are employed.</li> <li>• Automation is widely employed.             <ul style="list-style-type: none"> <li>- 50 percent of all controls are technical controls and 100 percent of these are automated.</li> <li>- Specific IT activities are automated.</li> </ul> </li> <li>• Policy-in and audit-out for technical controls is managed.</li> <li>• IT change controls and unauthorized change prevention are implemented.</li> <li>• Monitoring, measurement, and reporting occur from continuously to once a month.</li> </ul>
---

*Source: IT Policy Compliance Group, 2008*

**Table 4. Culture, budgeting, and spending**

Culture and budgeting	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
View of IT contribution to the organization	Not measured	IT is viewed as a utility expense and structured as such.	IT is primarily viewed as a utility expense, with specific projects for business growth.	IT is viewed as a utility expense and enabler of business growth.	IT is structured as an expense, with targets established for business growth.	IT is viewed as an enabler of business growth.
IT budgeting, spending, and focus	Not measured	IT spending is done from business units only.	Business units retain ownership of major applications. IT is responsible for infrastructure.	Most IT spending on IT is done by central IT headquarters only.	Business units purchase from vetted lists and IT is responsible for maintaining existing services.	Spending and budgets for IT are shared between business units and IT headquarters based on balanced scorecard.

*Source: IT Policy Compliance Group, 2008*

**Table 5. Business metrics, financial rewards, and risks**

Business outcomes	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Customer satisfaction	Not measured	8.7% lower	4.4% lower	No change	4.4% higher	8.7% higher
Customer retention	Not measured	6.3% lower	3.7% lower	No change	3.7% higher	7.3% higher
Revenues	Not measured	8.5% lower	4.3% lower	No change	4.3% higher	8.5% higher
Expenses	Not measured	6.4% lower	3.2% lower	No change	3.2% higher	6.4% higher
Profits	Not measured	6.9% lower	3.5% lower	No change	3.5% higher	6.9% higher

Source: IT Policy Compliance Group, 2008

**Table 6. Financial losses and risks**

Loss and risk	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Capital loss from data loss or theft	Approaches 10% of revenue, depending on firm size	Around 8% of revenue, depending on firm size	Around 6.5% of revenue, depending on firm size	Around 5% of revenue, depending on firm size	Around 3% of revenue, depending on firm size	Around 0.5% of revenue, depending on firm size
Frequency of capital loss from the loss or theft of sensitive data	Once every half-year to once every 10 years, depending on firm size	Once every year to once every 16 years, depending on firm size	Once every year to once every 25 years, depending on firm size	Once every 1.5 years to once every 45 years, depending on firm size	Once every 2.5 years to once every 77 years, depending on firm size	Once every 13 years to once every 800 years, depending on firm size
Capital loss from IT-based business disruptions	3–30% of revenue, depending on operational impact	1–9% of revenue, depending on operational impact	0.4–4% of revenue, depending on operational impact	0.1–1% of revenue, depending on operational impact	0.08–0.8% of revenue, depending on operational impact	0.03–0.3% of revenue, depending on operational impact

Source: IT Policy Compliance Group, 2008

**Table 7. Business and financial risk indicators**

Indicators	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Number of annual losses or thefts of sensitive data annually	16 or more	12	8	6	4	2 or less
Number of business disruptions based on IT service disruptions	24 or more	14	9	5	4	2 or less
Hours to resume business operations after IT service disruptions	28 or more	14	8	5	4	3 or less
Total hours of downtime annually	672 or more	196	72	25	16	6 or less
Regulatory compliance deficiencies to correct to pass audit	16 or more	12	10	8	4	2 or less

Source: IT Policy Compliance Group, 2008

**Table 8. Third-party, outsourced, and offshored IT services**

IT services	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Maturity by percentage of IT services performed by third-party vendors, outsourced, or offshored	Not measured	Between 40% and 60% of all IT services are outsourced or offshored.	Between 60% and 80% of all IT services are outsourced or offshored.	Between 80% and 100% of all IT services are outsourced or offshored.	Between 20% and 40% of all IT services are outsourced or offshored.	Between 0% and 20% of all IT services are outsourced or offshored.

Source: IT Policy Compliance Group, 2008

**Table 9. Continuous Quality Improvement**

CQI	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Existence and completeness of CQI programs	Not measured.	CQI is nonexistent.	CQI is nonexistent.	CQI is implemented in ad-hoc fashion and not connected with business results.	CQI program implemented by senior management team for major business initiatives.	Integrated CQI program is implemented from balanced scorecard through operations.

Source: IT Policy Compliance Group, 2008

**Table 10. Behavior and use of frameworks**

	<b>Maturity level 1</b>	<b>Maturity level 2</b>	<b>Maturity level 3</b>	<b>Maturity level 4</b>	<b>Maturity level 5</b>
Behavior and usage within IT operations, IT assurance, and IT audit	Four to five different frameworks are consulted but none are adopted as standards for use with IT operations, IT assurance, and IT audit.	Two to three different frameworks are consulted as the organization narrows down what it considers “best practices” for use with IT operations.	Organization attempts to standardize on one to two industry frameworks for use with IT operations, IT assurance, and IT audit.	List of frameworks is expanded to develop own framework to more effectively manage challenges within IT operations, IT assurance, and IT audit.	Own framework for IT operations, IT assurance, and IT audit is mapped to four or five different frameworks for managing risk, regulatory compliance, and business rewards.
Behavior within IT management	None are consulted or adopted.	Project management skills are emphasized, but no framework adoption occurs.	Frameworks for project management are adopted to deliver technology solutions.	Frameworks for business management, project management, and portfolio management are implemented to manage business rewards.	Frameworks for business management, project management, portfolio management, capability management, and quality improvement are implemented to balance reward and risk.

*Source: IT Policy Compliance Group, 2008*

**Table 11. Employee training and education**

	<b>Maturity level 1</b>	<b>Maturity level 2</b>	<b>Maturity level 3</b>	<b>Maturity level 4</b>	<b>Maturity level 5</b>
Training and education about company policies	Is left to the discretion of hiring managers.	Is delivered to employees upon hiring and documented in employee handbook.	Is delivered to all employees as part of onsite and required manager training programs, and is typically delivered once per year.	New programs dealing with legal and regulatory requirements are delivered as part of core curriculum. Delivery method starts to include Web- and computer-assisted training.	Formalized training program is implemented with Web- and computer-assisted course and policy curriculum, with multiple courses delivered every year.

**Table 12, Employee training and education**

Primary focus areas for employee training	Ethics and code of conduct Handling conflicts of interest	Ethics and code of conduct Handling conflicts of interest IT compliance, security, and data protection policies	Ethics and code of conduct Discrimination and harassment Handling conflicts of interest IT compliance, security, and data protection policies	Ethics and code of conduct IT compliance, security, and data protection policies Regulatory policies and procedures Discrimination and harassment Handling conflicts of interest Financial reporting and insider trading	Ethics and code of conduct IT compliance, security, and data protection policies Regulatory policies and procedures Discrimination and harassment Handling conflicts of interest Emergency response and restoration Financial reporting and insider trading Handling legal requests and summonses for information
---	--	---	--	---	--

Source: IT Policy Compliance Group, 2008

**Table 13. Spending on IT assurance and audit**

	<b>Maturity level 1</b>	<b>Maturity level 2</b>	<b>Maturity level 3</b>	<b>Maturity level 4</b>	<b>Maturity level 5</b>
Spending on IT assurance and audit as a percentage of the IT budget	5.2% to 7.4%	6.4% to 8.6%	7.4% to 9.6%	8.6% to 10.6%	9.6% to 11.6%

Source: IT Policy Compliance group, 2008

**Table 14. Actions to improve results**

	<b>Maturity level 1</b>	<b>Maturity level 2</b>	<b>Maturity level 3</b>	<b>Maturity level 4</b>	<b>Maturity level 5</b>
Actions taken to improve control objectives for IT GRC	Audit-based to pass the primary audit.	Audit-based to pass multiple audits.	Mixture of organizational policies to pass multiple audits.	Common policies and control objectives across multiple audits.	Policies and control objectives are rationalized based on business risks.
Actions taken to improve controls for IT GRC	Dominant manual and procedural controls to pass audit are documented.	Manual procedures and controls are rationalized against policies and control objectives.	Manual and technically automated procedures and controls for highest business risks are identified.	Mix of manual, procedural, and technical controls is changed. Modifications are documented through multiple audits.	Most technical procedures are fully automated. High-cost, low-value manual procedures are fully automated.
Organizational actions taken to improve IT GRC results	Evidence about conformance with policies is gathered to pass the primary audit. Gaps in procedures and IT general controls are fixed to pass audit. Rules and responsibilities of policy owners are established. Self-assessments of mostly manual procedural controls are conducted to pass audits. Employee training is left to individual managers.	Evidence about conformance with policies is gathered to pass multiple audits. Gaps in procedural controls and IT general controls are fixed to pass multiple audits. Rules and responsibilities of policy owners are established. Self-assessments of mostly manual procedural controls are conducted to pass audits. Employee training is paper-based in employee manuals.	Self-assessments of procedural controls are conducted. Gaps in procedures and IT general controls are fixed to pass audit. Rules and responsibilities of policy owners are established. Evidence about conformance with policies is gathered to pass audits. Employee training is paper-based in employee manuals.	Self-assessments of procedural controls are conducted. Monitoring and measurement of technical controls are being automated. Gaps in procedural controls and IT general controls are fixed to pass multiple audits. Policy owners are responsible for authorizing access to IT resources and employee training is a mix of electronic, paper, and instructor-led.	Self-assessments of procedural controls are conducted. Monitoring and measurement of technical controls are fully automated. The collection of audit data and remediation of gaps are automated. Controls, frameworks, policies, and control objectives are mapped to one another. Consistent IT configurations are employed and enforced. Policy owners are responsible for authorizing access to IT resources and employee training is electronic.

Source: IT Policy Compliance Group, 2008

**Table 15. Policies, objectives, and controls**

	<b>Maturity level 1</b>	<b>Maturity level 2</b>	<b>Maturity level 3</b>	<b>Maturity level 4</b>	<b>Maturity level 5</b>
Number of control objectives	82	70	58	45	31
Basis for control objectives	An amalgam of audit control statements, recommendations from auditors, and financial reporting risks.	An amalgam of audit control statements, recommendations from auditors, and financial reporting risks.	A mixture of recommendations from internal audit, finance, and IT.	A mixture of recommendations from internal audit, IT audit, IT assurance, and legal.	Based on ongoing risk assessments conducted across the organization covering finance, legal, regulatory, IT, and other organizational risks.
Number of controls	45	60	76	95	115
Proportion of manual controls	72%	66%	60%	53%	48%
Proportion of automated technical controls	28%	34%	40%	47%	52%
Proportion of technical controls that are fully automated	3%	8%	23%	49%	96%
Basis for controls	Whatever manual procedures and technical controls are available and recommendations of auditors.	Whatever manual procedures and technical controls are available and recommendations of auditors.	Business risks from internal audit, finance, IT, and recommendations of auditors.	Consensus of business risks from leadership and audit committee.	Consensus of business risks from leadership and audit committee.

*Source: IT Policy Compliance Group, 2008*

**Table 16. Frequency of measurement, assessment, and reporting**

	<b>Maturity level 1</b>	<b>Maturity level 2</b>	<b>Maturity level 3</b>	<b>Maturity level 4</b>	<b>Maturity level 5</b>
Frequency of IT general controls assessment, measurement, monitoring, and reporting for regulatory audit	Once every 300 days	Once every 222 days	Once every 105 days	Once every 45 days	Once every 17 days
Frequency of IT general controls assessment, measurement, monitoring, and reporting for data protection	Once every 300 days	Once every 210 days	Once every 90 days	Once every 29 days	Once every 4 days
Percentage of IT general controls routinely assessed, measured, monitored, and reported	30%	40%	50%	60%	70%

Source: IT Policy Compliance Group, 2008

**Table 17. Change management and prevention**

	<b>Maturity level 1</b>	<b>Maturity level 2</b>	<b>Maturity level 3</b>	<b>Maturity level 4</b>	<b>Maturity level 5</b>
IT change management program	Change management for IT is not considered a priority or is unknown.	Change management is limited to PCs and financial systems to pass audits.	Change management for critical IT resources is identified and more are implemented for critical IT resources.	Change management is Implemented for critical IT resources.	Change management is implement for all IT resources.
Unauthorized changes to IT resources automatically prevented	25%	35%	45%	60%	75%
Unauthorized changes to IT resources managed by exception	75%	65%	55%	40%	25%

*Source: IT Policy Compliance Group, 2008*