



Example information security metrics

Version 2 1st March 2009

Introduction

Most of the metrics pages that follow were originally documented in a metrics workshop held by [ISACA in Wellington, New Zealand](#). Subsequently they have been updated with further ideas from a [presentation/tutorial by Dan Geer](#), the [book by Andrew Jaquith](#), and continued head-scratching by [Gary Hinson](#).

Scope

The metrics outlined below are merely examples or suggestions of information security metrics that we believe are both pragmatic and useful. They are sorted according to the most relevant sections of ISO/IEC 27002, partly because we feel it is appropriate to aim for coverage of all sections.

Purpose

This document is meant to help those who are implementing or have implemented the ISO/IEC 27000-series information security management standards, or indeed any organization that wants to improve its management of information security, to think up useful information security metrics. Like the ISO/IEC standards, it is generic and needs to be tailored to each organization's specific requirements. The metrics described here are merely examples to illustrate how various kinds of information security objective can be measured in order to drive systematic security improvements. The metrics you actually need are determined by factors such as existing metrics practices; the availability and cost of collecting and analyzing additional measurement data; your security objectives and priorities; the maturity of your Information Security Management System; and so forth. All we ask in return is that if you find this paper useful, and especially if you design additional worthwhile information security metrics, you share your ideas with others, ideally via the [ISO27k Implementers' Forum](#).

Copyright



This work is copyright © 2009, [ISO27k Implementers' Forum](#), some rights reserved. It is licensed under the [Creative Commons Attribution-Noncommercial-Share Alike 3.0 License](#). You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum (www.ISO27001security.com) and the original authors and contributors identified in the introduction, and (c) derivative works are shared under essentially the same open terms as this.

Title/name of metric	Risk exposure		
Primary customer	Executives		
Information source/s	Risk analyses		
How calculated	Sum of realistic worst-case impact costs for all unmitigated information security risks against critical information systems		
Frequency	Annual		
Rationale for measuring this	Although it is inevitable that not all information security risks can be fully mitigated, the value of unmitigated risks indicates the extent to which the organization remains exposed.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 <i>Information security governance</i> 7 <i>Asset mgmt</i>	8 HR 9 Physical security 10 Comms/Ops mgmt 11 Access control	12 SDLC 13 Incident mgmt 14 Continuity mgmt 15 Compliance
Nature of metric	Leading / Lagging / <u>Semi</u> Soft / <u>Hard</u> / Semi Objective / Subjective / <u>Semi</u> <u>Absolute</u> / Relative (trend) / Semi <u>Confidentiality / Integrity / Availability</u>		
Alternative metrics considered			
Notes	Double-counting could be an issue unless potential exposures are rationalized. "Realistic worst case impact costs" would need to be defined as a policy matter unless all values are independently assessed and normalized (e.g. by Finance or Risk Management?).		

Title/name of metric	information security efficiency		
Primary customer	Executives		
Information source/s	Expenditure from Finance; incidents from Help Desk		
How calculated	Estimated total cost of security incidents suffered in year / total security expenditure in year		
Frequency	Annual		
Rationale for measuring this	it is reasonable for management to expect increased expenditure on information security to reduce the costs actually incurred by security incidents, and vice versa.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 <u>Information security governance</u> 7 Asset mgmt	8 HR 9 Physical security 10 Comms/Ops mgmt 11 Access control	12 SDLC 13 Incident mgmt 14 Continuity mgmt 15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi Objective / Subjective / Semi Soft / <u>Hard</u> / Semi <u>Absolute</u> / Relative (trend) / Semi <u>Confidentiality / Integrity / Availability</u>		
Alternative metrics considered			
Notes	Neither the incident nor the security costs are easy to measure accurately but so long as the ground rules are established (e.g. by Finance) and remain consistent year-to-year, it should be possible for management to identify the linkage between discretionary security expenditure and non-discretionary security losses.		

Title/name of metric	Customer security sophistication index		
Primary customer	general manager of ebusiness function		
Information source/s	Customer survey		
How calculated	survey using % ranges and Key indicators against predetermined criteria (e.g. use of antivirus)		
Frequency	Annual		
Rationale for measuring this	Customer insecurities could introduce viruses, create data integrity problems and result in unauthorized disclosure of information affecting the organization. Less sophisticated/security aware customers are likely to have less effective security controls.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt	8 HR	12 SDLC
	5 Security policy	9 Physical security	13 Incident mgmt
	6 Infosec governance	10 Comms/Ops mgmt	14 Continuity mgmt
	7 Asset mgmt	11 Access control	15 Compliance
Nature of metric	Leading / Lagging / Semi Objective / Subjective / Semi Soft / Hard / Semi Absolute / Relative (trend) / Semi Confidentiality / Integrity / Availability		
Alternative metrics considered	general security surveys (not specific to customers)		
Notes	Might be interesting to compare the 'customer security sophistication index' to the number of ebusiness security incidents that appear to result from customer security issues. if the survey questionnaire is reviewed/updated annually, new risks could be reflected. Security awareness activities targeted at customers should noticeably improve this index.		

Title/name of metric	Security clearance lag		
Primary customer	HR Manager, Information Security Manager, CIO		
Information source/s	HR system		
How calculated	Average #working days between approval of appointment and security clearance being granted or denied for new employees during the reporting period		
Frequency	Measured and reported quarterly		
Rationale for measuring this	if employees are appointed "pending full clearance", the longer it takes to complete the police checks the greater the exposure to fraud, theft or other criminal acts by unsuitable employees.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> Subsidiary	4 Risk mgmt	<u>8 HR</u>	12 SDLC
	5 Security policy	9 Physical security	13 Incident mgmt
	6 Infosec governance	10 Comms/Ops mgmt	14 Continuity mgmt
	7 Asset mgmt	11 Access control	15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi Soft / <u>Hard</u> / Semi <u>Objective</u> / Subjective / Semi Absolute / Relative (trend) / Semi Confidentiality / Integrity / Availability		
Alternative metrics considered	#employees pre-cleared/#appointed without clearance		
Notes	<p>Might be interesting to breakdown or analyze the figures according to the nature of job role (e.g. if appointments to highly responsible positions require express clearance?).</p> <p>Process delays outside the organization's control will heavily influence this metric, although process improvements may help.</p>		

Title/name of metric	Security roles and responsibilities		
Primary customer	HR Director		
Information source/s	HR and Procurement - data from contractual review		
How calculated	<p>% of workers whose security responsibilities have been adequately:</p> <p>(a) determined</p> <p>(b) fully specified in employment or service contracts, job/role descriptions, procedures etc.</p>		
Frequency	6 monthly		
Rationale for measuring this	if security is truly "everybody's responsibility", then it ought to be properly specified and documented in everybody's employment or service contracts, job/role descriptions, procedures etc.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt	8 HR	12 SDLC
	5 Security policy	9 Physical security	13 Incident mgmt
	6 Information security governance	10 Comms/Ops mgmt	14 Continuity mgmt
	7 Asset mgmt	11 Access control	15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi Objective / Subjective / <u>Semi Absolute</u> / Relative (trend) / Semi Soft / Hard / <u>Semi Confidentiality / Integrity / Availability</u>		
Alternative metrics considered			
Notes	A breakdown of the figures by department may help stimulate improvements ...		

Title/name of metric	Access to controlled facilities		
Primary customer	Facilities management, CIO		
Information sources	Card access control system logs		
How calculated	#unsuccessful / #successful access attempts to controlled areas		
Frequency	Daily collection, monthly reporting		
Rationale for measuring this	if people are "rattling the doorlocks", attempting access to controlled areas, this indicates a lax attitude towards physical security.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 Infosec governance 7 Asset mgmt	8 HR 9 Physical security 10 Comms/Ops mgmt 11 Access control	12 SDLC 13 Incident mgmt 14 Continuity mgmt 15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi Soft / <u>Hard</u> / Semi Objective / Subjective / Semi Absolute / Relative (trend) / Semi Confidentiality / Integrity / Availability		
Alternative metrics considered	Reports of unauthorized visitors		
Notes	Further analysis of failed accesses may indicate systematic issues such as people not having the correct access rights, using shared cards etc. should be coupled with analysis of successful accesses to secure areas (e.g. confirming that all who access the area should in fact have that level of access).		

Title/name of metric	Network capacity												
Primary customer	CIO												
Information source/s	User activity; audit logs; #IDs; IT Help/Service Desk reports; transaction logs; previous trends; change requests; statutory obligations												
How calculated	Used / Available network capacity x 100%												
Frequency	Daily collection, monthly reporting												
Rationale for measuring this	Ensure availability of sufficient network capacity to meet current business demands (with trends analysis for future projections)												
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	<table border="0"> <tr> <td>4 Risk mgmt</td> <td>8 HR</td> <td>12 SDLC</td> </tr> <tr> <td>5 Security policy</td> <td>9 Physical security</td> <td>13 Incident mgmt</td> </tr> <tr> <td>6 Infosec governance</td> <td>10 Comms/Ops mgmt</td> <td>14 Continuity mgmt</td> </tr> <tr> <td>7 Asset mgmt</td> <td>11 Access control</td> <td>15 Compliance</td> </tr> </table>	4 Risk mgmt	8 HR	12 SDLC	5 Security policy	9 Physical security	13 Incident mgmt	6 Infosec governance	10 Comms/Ops mgmt	14 Continuity mgmt	7 Asset mgmt	11 Access control	15 Compliance
4 Risk mgmt	8 HR	12 SDLC											
5 Security policy	9 Physical security	13 Incident mgmt											
6 Infosec governance	10 Comms/Ops mgmt	14 Continuity mgmt											
7 Asset mgmt	11 Access control	15 Compliance											
Nature of metric	<p>Leading / Lagging / <u>Semi</u> Objective / Subjective / Semi</p> <p>Soft / <u>Hard</u> / Semi Absolute / <u>Relative (trend)</u> / Semi</p> <p>Confidentiality / Integrity / <u>Availability</u></p>												
Alternative metrics considered	<p>Capacity of network connections for essential web servers.</p> <p>#named/registered web services users.</p> <p>#Failed/successful web services login attempts.</p> <p>SLA statistics if web services are outsourced.</p>												
Notes	Presentation using "highest-mean-lowest" bars, with commentary on any significant changes from the norm.												

Title/name of metric	information security risk mitigation		
Primary customer	CIO		
Information source/s	Change management systems, vulnerability tests etc.		
How calculated	<p>% of critical business applications that are:</p> <ol style="list-style-type: none"> 1. Running on fully patched and hardened systems 2. Fully physically secured 3. Fully risk assessed 4. Fully security tested and certified 5. Fully supported by backups and recovery plans 		
Frequency	Quarterly		
Rationale for measuring this	These high-level metrics indicate the extent to which important drivers of system security are being achieved in practice		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 Information security governance 7 Asset mgmt	8 HR 9 Physical security 10 Comms/Ops mgmt 11 Access control	12 SDLC 13 Incident mgmt 14 Continuity mgmt 15 Compliance
Nature of metric	<p>Leading / <u>Lagging</u> / Semi Soft / Hard / <u>Semi</u></p> <p>Objective / Subjective / <u>Semi</u> Absolute / Relative (trend) / <u>Semi</u> <u>Confidentiality / Integrity / Availability</u></p>		
Alternative metrics considered			
Notes	"Fully" could perhaps be defined for each part of this metric to mean "As specified in the relevant policies, SLAs, contracts or system security specifications"		

Title/name of metric	Privileged users
Primary customer	information Asset owners
Information source/s	IT
How calculated	Proportion of privileged user IDs per critical application system
Frequency	Quarterly
Rationale for measuring this	Privileged users have rights that allow them to overrule security controls that apply to ordinary/non-privileged users. Bringing this figure under control contributes to securing the systems by reducing opportunities for abuse.
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 Information security governance 7 Asset mgmt 8 HR 9 Physical security 10 Comms/Ops mgmt <u>11 Access control</u> 12 SDLC 13 Incident mgmt 14 Continuity mgmt 15 Compliance
Nature of metric	<u>Leading</u> / Lagging / Semi <u>Soft</u> / Hard / Semi <u>Objective</u> / Subjective / Semi Absolute / <u>Relative (trend)</u> / Semi Confidentiality / <u>Integrity</u> / Availability
Alternative metrics considered	
Notes	it is feasible for management to set a target proportion for all systems, and to rank systems by the proportions achieved in practice in order to stimulate improvement of the worst.

Title/name of metric	Payroll data quality		
Primary customer	Senior management team		
Information source/s	Payroll database logs and system change records		
How calculated	$\frac{(\# \text{exceptions and corrections processed during the period} - \# \text{legitimate data changes})}{\# \text{records in the database}} \times 100\%$		
Frequency	Weekly collection quarterly reporting		
Rationale for measuring this	Measures data integrity failures (completeness, accuracy, timeliness) in an important database where the consequences of data errors may be significant		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt	8 HR	<u>12 SDLC</u>
	5 Security policy	9 Physical security	13 Incident mgmt
	6 Infosec governance	10 Comms/Ops mgmt	14 Continuity mgmt
	7 Asset mgmt	11 Access control	15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi <u>Objective</u> / Subjective / Semi Soft / <u>Hard</u> / Semi Absolute / <u>Relative (trend)</u> / Semi Confidentiality / <u>Integrity</u> / Availability		
Alternative metrics considered	Delayed updates to personnel records		
Notes	<p>Some payroll data changes are more significant than others but this metric simply counts the number of data corrections to assess the accuracy level. Better automated or manual data entry controls should reduce the number of errors having to be corrected.</p> <p>The same metric can be applied to any database, ERP or similar systems, and compared between systems.</p>		

Title/name of metric	<i>Code complexity</i>												
Primary customer	<i>CIO</i>												
Information source/s	<i>McCabe Cyclomatic statistics from development environments</i>												
How calculated	<i>1 / McCabe cyclomatic figure</i>												
Frequency	<i>once per developed system</i>												
Rationale for measuring this	<i>Complexity is the enemy of security, so reducing complexity (to increase this metric) is a worthwhile security goal</i>												
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	<table border="0"> <tr> <td>4 Risk mgmt</td> <td>8 HR</td> <td><u>12 SDLC</u></td> </tr> <tr> <td>5 Security policy</td> <td>9 Physical security</td> <td>13 Incident mgmt</td> </tr> <tr> <td>6 Information security governance</td> <td>10 Comms/Ops mgmt</td> <td>14 Continuity mgmt</td> </tr> <tr> <td>7 Asset mgmt</td> <td>11 Access control</td> <td>15 Compliance</td> </tr> </table>	4 Risk mgmt	8 HR	<u>12 SDLC</u>	5 Security policy	9 Physical security	13 Incident mgmt	6 Information security governance	10 Comms/Ops mgmt	14 Continuity mgmt	7 Asset mgmt	11 Access control	15 Compliance
4 Risk mgmt	8 HR	<u>12 SDLC</u>											
5 Security policy	9 Physical security	13 Incident mgmt											
6 Information security governance	10 Comms/Ops mgmt	14 Continuity mgmt											
7 Asset mgmt	11 Access control	15 Compliance											
Nature of metric	<p><u>Leading</u> / Lagging / Semi Soft / <u>Hard</u> / Semi</p> <p><u>Objective</u> / Subjective / Semi <u>Absolute</u> / Relative (trend) / Semi <u>Confidentiality / Integrity / Availability</u></p>												
Alternative metrics considered	<i>1 / lines of code squared (a less sophisticated measure of code complexity)</i>												
Notes													

Title/name of metric	Proportion of security incidents		
Primary customer	Information Security Managers, CIO, CEO & Board		
Information source/s	IT Help/Service Desk call logging & tracking systems		
How calculated	#security incidents / #all incidents reported in reporting period		
Frequency	Weekly (ISMD), Monthly (CIO), quarterly (CEO & Board)		
Rationale for measuring this	We would expect security awareness activities to drive up the reporting of security incidents		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 Infosec governance 7 Asset mgmt	8 HR 9 Physical security 10 Comms/Ops mgmt 11 Access control	12 SDLC 13 Incident mgmt 14 Continuity mgmt 15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi Objective / Subjective / <u>Semi</u> Soft / Hard / <u>Semi</u> Absolute / <u>Relative (trend)</u> / Semi Confidentiality / Integrity / Availability		
Alternative metrics considered	Other security awareness metrics e.g. proportion of employees that have completed some form of security awareness training during the period, or have signed their acceptance of security policies and related obligations.		
Notes	Would require care to ensure that security-related incidents are correctly categorized by the Help Desk. Does not take account of the differing severity of security incidents.		

Title/name of metric	Days since a serious security incident		
Primary customer	Entire workforce (security awareness)		
Information source/s	IT Help/Service Desk incident logs		
How calculated	#days since an information security incident judged by management to have caused "serious" business impact		
Frequency	Daily collection and reporting		
Rationale for measuring this	Modern analogue of the old "Days since a lost time safety incident" boards outside factories		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt	8 HR	12 SDLC
	5 Security policy	9 Physical security	<u>13 Incident mgmt</u>
	6 Infosec governance	10 Comms/Ops mgmt	14 Continuity mgmt
	7 Asset mgmt	11 Access control	15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi Soft / <u>Hard</u> / Semi <u>Objective</u> / Subjective / Semi <u>Absolute</u> / Relative (trend) / Semi Confidentiality / Integrity / Availability		
Alternative metrics considered	"Security status" or "risk level" (both subjective assessments)		
Notes	"Serious" may have to be defined formally, perhaps using example incidents or costs that would trigger a reset of the day count. The metric could be reported by business unit.		

Title/name of metric	Coordinated Business Continuity Plans		
Primary customer	Security management & executives		
Information source/s	All business units or contingency planning function		
How calculated	Count number of BCPs that have been signed to denote review and acceptance by the heads of all relevant business functions invoked in the plans		
Frequency	Collect & report quarterly in year 1, then half-yearly in year 2, then annually (as continuity processes mature)		
Rationale for measuring this	Business continuity plans for any department typically call upon other departments (e.g. IT) but coordination of plans between departments is not automatically guaranteed. This metric checks that plans have been coordinated with and accepted by all the business functions they invoke.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 Information security governance 7 Asset mgmt	8 HR 9 Physical security 10 Comms/Ops mgmt 11 Access control	12 SDLC 13 Incident mgmt 14 Continuity mgmt 15 Compliance
Nature of metric	Leading / Lagging / Semi Soft / Hard / Semi Objective / Subjective / Semi* Absolute / Relative (trend) / Semi Confidentiality / Integrity / Availability		
Alternative metrics considered	Number of BCPs successfully tested/exercised		
Notes	* The metric itself is objective but the degree to which signatories review and approve the plans may vary		

Title/name of metric	<i>Business recovery cycle time</i>		
Primary customer	<i>Security management & executives</i>		
Information source/s	<i>DR and business continuity tests</i>		
How calculated	<i>Measure/estimate time from start or restoration (measured from the invocation of a disaster) to operation of recovered critical business processes, (Measured at the point the recovered processes are signed-off by the business customers as recovered)</i>		
Frequency	<i>Collect at each DR/BCP test</i>		
Rationale for measuring this	<i>Critical business functions, by definition, cost money for as long as they are inoperable, so minimizing this time is a worthwhile goal for DR and BCP.</i>		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 Information security governance 7 Asset mgmt	8 HR 9 Physical security 10 Comms/Ops mgmt 11 Access control	12 SDLC 13 Incident mgmt <u>14 Continuity mgmt</u> 15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi Soft / <u>Hard</u> / Semi <u>Objective</u> / Subjective / Semi <u>Absolute</u> / Relative (trend) / Semi Confidentiality / Integrity / <u>Availability</u>		
Alternative metrics considered			
Notes			

Title/name of metric	Personal device security		
Primary customer	Security manager / committee		
Information source/s	IT Help/Service Desk incident log + automated system logs (e.g. antivirus and antispymware logs)		
How calculated	$\# \text{ of security incidents} / \# \text{ personal devices} \times 100\%$		
Frequency	Collect daily Report monthly or quarterly		
Rationale for measuring this	Monitor security risks to personal devices (PDAs, laptops, mobile phones etc) that often fall outside the purview of the information security management system, yet carry sensitive & valuable data. Identify education/awareness targets and security issues. Ensure policy compliance.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <u>Subsidiary</u>	4 Risk mgmt	8 HR	12 SDLC
	5 Security policy	9 Physical security	13 Incident mgmt
	6 Infosec governance	10 Comms/Ops mgmt	14 Continuity mgmt
	7 Asset mgmt	11 Access control	15 Compliance
Nature of metric	Leading / <u>Lagging</u> / Semi Soft / <u>Hard</u> / Semi <u>Objective</u> / Subjective / Semi Absolute / <u>Relative (trend)</u> / Semi <u>Confidentiality</u> / Integrity / Availability		
Alternative metrics considered	Automated compliance checks using automated controls e.g. antivirus, security configuration checkers		
Notes			

Title/name of metric	Web abuse		
Primary customer	HR Department		
Information source/s	internet filtering software		
How calculated	#non-acceptable sites / #acceptable sites accessed or attempted access during the period		
Frequency	Collected daily, reported monthly		
Rationale for measuring this	Policy compliance issue: employees accessing (or attempting to access) "unacceptable" sites increase the possibility of malware infections, data theft, prosecution for porn & unlicensed software etc.		
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	4 Risk mgmt 5 Security policy 6 Infosec governance 7 Asset mgmt	8 HR 9 Physical security 10 Comms/Ops mgmt 11 Access control	12 SDLC 13 Incident mgmt 14 Continuity mgmt <u>15 Compliance</u>
Nature of metric	Leading / <u>Lagging</u> / Semi Objective / Subjective / <u>Semi</u> Soft / <u>Hard</u> / Semi Absolute / Relative (trend) / <u>Semi</u> Confidentiality / Integrity / Availability		
Alternative metrics considered	Separately measure and report successful vs blocked accesses to unacceptable sites.		
Notes	<p>Could be reported by department to department managers, allowing benchmarking comparisons.</p> <p>Assumes "acceptability" of websites has been defined in policy and web filtering software configured accordingly. Also assumes tor and similar proxy sites are blocked (could usefully be monitored too!).</p> <p>Metric should improve with user awareness training and follow-up activities by management.</p>		

[Blank form to use in your own metrics workshop!]

Title/name of metric													
Primary customer													
Information source/s													
How calculated													
Frequency													
Rationale for measuring this													
Relevant section/s of ISO/IEC 27002 <u>Main</u> <i>Subsidiary</i>	<table> <tr> <td>4 Risk mgmt</td> <td>8 HR</td> <td>12 SDLC</td> </tr> <tr> <td>5 Security policy</td> <td>9 Physical security</td> <td>13 Incident mgmt</td> </tr> <tr> <td>6 Information security governance</td> <td>10 Comms/Ops mgmt</td> <td>14 Continuity mgmt</td> </tr> <tr> <td>7 Asset mgmt</td> <td>11 Access control</td> <td>15 Compliance</td> </tr> </table>	4 Risk mgmt	8 HR	12 SDLC	5 Security policy	9 Physical security	13 Incident mgmt	6 Information security governance	10 Comms/Ops mgmt	14 Continuity mgmt	7 Asset mgmt	11 Access control	15 Compliance
4 Risk mgmt	8 HR	12 SDLC											
5 Security policy	9 Physical security	13 Incident mgmt											
6 Information security governance	10 Comms/Ops mgmt	14 Continuity mgmt											
7 Asset mgmt	11 Access control	15 Compliance											
Nature of metric	<table> <tr> <td>Leading / Lagging / Semi</td> <td>Objective / Subjective / Semi</td> </tr> <tr> <td>Soft / Hard / Semi</td> <td>Absolute / Relative (trend) / Semi</td> </tr> <tr> <td></td> <td>Confidentiality / Integrity / Availability</td> </tr> </table>	Leading / Lagging / Semi	Objective / Subjective / Semi	Soft / Hard / Semi	Absolute / Relative (trend) / Semi		Confidentiality / Integrity / Availability						
Leading / Lagging / Semi	Objective / Subjective / Semi												
Soft / Hard / Semi	Absolute / Relative (trend) / Semi												
	Confidentiality / Integrity / Availability												
Alternative metrics considered													
Notes													