

Title/name of metric	<i>Coordinated Business Continuity Plans</i>		
Primary customer	<i>Security management & executives</i>		
Information source/s	<i>All business units or contingency planning function</i>		
How calculated	<i>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</i>		
Frequency	<i>Collect & report quarterly in year 1, then half-yearly in year 2, then annually (as continuity processes mature)</i>		
Rationale for measuring this	<i>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.</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 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	<i>Number of BCPs successfully tested/exercised</i>		
Notes	<i>* The metric itself is objective but the degree to which signatories review and approve the plans may vary</i>		

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 antispyware 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 Main <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 Soft / Hard / Semi Objective / Subjective / Semi Absolute / Relative (trend) / Semi Confidentiality / Integrity / Availability		
Alternative metrics considered	Automated compliance checks using automated controls e.g. antivirus, security configuration checkers		
Notes			

Title/name of metric	Payroll data quality												
Primary customer	Senior management team												
Information source/s	Payroll database logs and system change records												
How calculated	$(\# \text{exceptions and corrections processed during the period} - \# \text{legitimate data changes}) / \# \text{records in the database} \times 100\%$												
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> <u>Subsidiary</u>	<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 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	<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
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	<table border="0"> <tr> <td>Leading / <u>Lagging</u> / Semi</td> <td><u>Objective</u> / Subjective / Semi</td> </tr> <tr> <td>Soft / <u>Hard</u> / Semi</td> <td>Absolute / <u>Relative (trend)</u> / Semi</td> </tr> <tr> <td></td> <td>Confidentiality / <u>Integrity</u> / Availability</td> </tr> </table>	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						
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	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 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 <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	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	$Used / Available\ network\ capacity \times 100\%$		
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>	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 / Lagging / <u>Semi</u> Objective / Subjective / Semi Soft / <u>Hard</u> / Semi Absolute / <u>Relative (trend)</u> / Semi Confidentiality / Integrity / <u>Availability</u>		
Alternative metrics considered	Capacity of network connections for essential web servers. #named/registered web services users. #Failed/successful web services login attempts. SLA statistics if web services are outsourced.		
Notes	Presentation using "highest-mean-lowest" bars, with commentary on any significant changes from the norm.		

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 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 / <u>Subjective</u> / Semi <u>Soft</u> / Hard / Semi Absolute / <u>Relative (trend)</u> / Semi Confidentiality / <u>Integrity</u> / Availability		
Alternative metrics considered	general security surveys (not specific to customers)		
Notes	<p>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.</p> <p>if the survey questionnaire is reviewed/updated annually, new risks could be reflected.</p> <p>Security awareness activities targeted at customers should noticeably improve this index.</p>		

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>		

Title/name of metric	<i>Access to controlled facilities</i>		
Primary customer	<i>Facilities management, CIO</i>		
Information sources	<i>Card access control system logs</i>		
How calculated	<i>#unsuccessful / #successful access attempts to controlled areas</i>		
Frequency	<i>Daily collection, monthly reporting</i>		
Rationale for measuring this	<i>if people are "rattling the doorlocks", attempting access to controlled areas, this indicates a lax attitude towards physical security.</i>		
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 <i>Confidentiality</i> / Integrity / <i>Availability</i>		
Alternative metrics considered	<i>Reports of unauthorized visitors</i>		
Notes	<i>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).</i>		

Title/name of metric	Security clearance lag time		
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	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.		