

# ISO/IEC 27004:2016-12 (E)

## Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Structure and overview .....	1
5	Rationale .....	2
5.1	The need for measurement .....	2
5.3	Validity of results .....	3
5.4	Benefits .....	3
6	Characteristics .....	4
6.1	General .....	4
6.2	What to monitor .....	4
6.3	What to measure .....	5
6.4	When to monitor, measure, analyse and evaluate .....	6
6.5	Who will monitor, measure, analyse and evaluate .....	6
7	Types of measures .....	7
7.1	General .....	7
7.2	Performance measures .....	7
7.3	Effectiveness measures .....	8
8	Processes .....	9
8.1	General .....	9
8.2	Identify information needs .....	10
8.3	Create and maintain measures .....	11
8.3.1	General .....	11
8.3.2	Identify current security practices that can support information needs .....	11
8.3.3	Develop or update measures .....	12
8.3.4	Document measures and prioritize for implementation .....	13
8.3.5	Keep management informed and engaged .....	13
8.4	Establish procedures .....	14
8.5	Monitor and measure .....	14
8.6	Analyse results .....	15
8.7	Evaluate information security performance and ISMS effectiveness .....	15
8.8	Review and improve monitoring, measurement, analysis and evaluation processes .....	15
8.9	Retain and communicate documented information .....	15
Annex A (informative) An information security measurement model .....		17
Annex B (informative) Measurement construct examples .....		19
Annex C (informative) An example of free-text form measurement construction .....		57
Bibliography .....		58