情報セキュリティマネジメントシステム
ISMS (Information Security Management System)

① 情報資産に対する機密性、完全性、可用性を評価する。

機密性

資産価値	クラス	
1	公開	第三者に対してオープン
2	社外秘	組織内のみ
3	秘密	特定の関係者
4	極秘	ごく一部の関係者

完全性

資産価値	クラス	
1	低	改ざんに対して影響は小さい
2	中	改ざんに対して影響は大きい
3	高	改ざんに対して影響は深刻かつ重大

可用性

資産価値	クラス	
1	低	１日利用できなくても構わない（１日のシステム停止は OK）
2	中	営業時間内の利用は保障されている（１時間のシステム停止は OK）
3	高	１年のうち 99%以上は利用可能

② 情報資産に対する脅威とその大きさ調べて、その脅威に対する脆弱性の度合いを評価する。

脅威

大きさ	クラス	発生頻度
1	発生率 極小	10%以下
2	発生率 小	10～30%
3	発生率 中	30～50%
4	発生率 大	50%以上

脆弱性

度合い	クラス	
1	低	適切な管理がなされていて安全
2	中	管理策の追加等により改善の余地がある
3	高	全く管理がなされておらず脆弱である

③ 情報資産のリスク値を計算し、リスク水準を設定する。

【リスク値】

機密性、完全性、可用性について

（リスク値）＝（資産価値）×（脅威の大きさ）×（脆弱性の度合い）

【リスク水準】

機密性、完全性、可用性のリスク値の最大値の３分の１とする。

（機密性のリスク水準）＝４×４×３×（１／３）＝１６

（完全性のリスク水準）＝３×４×３×（１／３）＝１２

（機密性のリスク水準）＝３×４×３×（１／３）＝１２

④ 情報資産の機密性、完全性、可用性のリスク値が（一つでも）リスク水準を超えた場合は、何らかの対応（改善）を行い、リスク値がすべてリスク水準を超えないようにする。

以上のプロセス（評価・点検・改善）を定期的に実行し、情報セキュリティ（情報システムの安全性）を常に高めておく。

【例】 情報資産：ある企業で開発中の新製品に関する電子データ

① 情報資産に対して機密性、完全性、可用性を評価する。

資産価値： 機密性 ３、完全性 ３、可用性 ２

② 情報資産に対する脅威とその大きさを調べて、その脅威に対する脆弱性の度合いを評価する。

脅威：電子データを保存しているサーバへのウィルス攻撃 ⇒ 脅威の大きさ ３
脆弱性： ウィルス対策が全くなされていない ⇒ 脆弱性の度合い ３

③ 情報資産のリスク値を計算し、リスク水準を設定する。

機密性　（リスク値）３×３×３＝２７　（リスク水準）１６
完全性　（リスク値）３×３×３＝２７　（リスク水準）１２
可用性　（リスク値）２×３×３＝１８　（リスク水準）１２

④ 上記の場合、情報資産の機密性、完全性、可用性のリスク値が全てリスク水準を超えているので、何らかの対応（改善）を行う必要がある。
そこで、この企業は最新のウィルス対策ソフトをサーバに導入した。その結果、ウィルス攻撃という脅威に対する脆弱性の度合いが（当分の間は）１と評価される。リスク値の再計算を行うと、

機密性　（リスク値）３×３×１＝９　（リスク水準）１６
完全性　（リスク値）３×３×１＝９　（リスク水準）１２
可用性　（リスク値）２×３×１＝６　（リスク水準）１２

となり、全てのリスク値がリスク水準未満になっている。これにより（当分の間は）情報セキュリティが確保されることになる。