



INFOCHIEF®

Training & Consulting Services

## CẨM NANG QUẢN LÝ IT

CÁC HƯỚNG  
DẪN THỰC  
HÀNH QUẢN  
LÝ IT HIỆU  
QUẢ VÀ THỰC  
TIỄN NHẤT

# QUẢN LÝ BẢO MẬT & RỦI RO IT

*Phát triển năng lực quản lý IT toàn diện*

FREE ACCESS TO  
ONLINE TOOLS

## GIỚI THIỆU

Bất cứ sự cố nào cũng có thể xảy ra trong hệ thống IT, chính điều này luôn tạo ra một áp lực vô hình đối với người quản trị hệ thống CNTT trong doanh nghiệp. Để phòng tránh những sự cố này xảy ra, cần phải có quy trình đánh giá, đặt ra các tình huống tác động đối với hệ thống, xác định mức độ rủi ro, khả năng ảnh hưởng đến hoạt động kinh doanh của tổ chức doanh nghiệp. Từ đó xác định các biện pháp, cũng như những kịch bản ứng phó rủi ro hiệu quả.

Quản lý bảo mật thông tin và rủi ro IT là quyển sách hướng dẫn bao gồm các thủ tục, quy trình và chính sách bảo đảm an toàn cho IT. Nội dung biên soạn nằm trong phạm vi bảo mật hệ thống thông tin doanh nghiệp theo tiêu chuẩn ISO 27001:2005, tập trung vào xây dựng chính sách an toàn cho hệ thống thông tin, triển khai đào tạo nhận thức, bên cạnh đó là phần đánh giá khả năng rủi ro tài sản công nghệ và lập kế hoạch dự phòng và khôi phục thảm họa hệ thống (DRP). Từng phần của quyển sách là các hướng dẫn chi tiết, cụ thể dựa trên các biểu mẫu, ví dụ minh họa đa dạng, giúp người đọc có thể tự mình thực hành lập kế hoạch, xây dựng các chính sách và triển khai hiệu quả cho tổ chức IT.

Quản lý bảo mật thông tin và rủi ro IT là một trong số 10 quyển sách cẩm nang dành cho người làm quản lý IT trong doanh nghiệp cần phải có, mục tiêu các quyển sách này đều là các hướng dẫn chi tiết nhằm **Phát triển năng lực cho người quản lý IT**.

*Book 1. Lập kế hoạch chiến lược IT*

*Book 6. Lập kế hoạch ngân sách IT*

*Book 2. Lập kế hoạch dự án IT*

*Book 7. Quản lý mua sắm và nhà cung cấp IT*

*Book 3. Quản lý dịch vụ IT*

*Book 8. Quản lý bộ phận IT*

*Book 4. Quản lý tài sản IT*

*Book 9. Quản lý nhân viên IT*

*Book 5. Quản lý bảo mật thông tin và rủi ro IT*

*Book 10. 90 Ngày lãnh đạo IT*

Học viện Infochief cũng tổ chức khóa học 5 ngày về các nội dung này. Các bạn có thể xem chi tiết nội dung khóa học tại địa chỉ website của học viện infochief:

<http://infochief.com.vn/Infochief-course-IT-Management-Skills.htm>

**Paul Huỳnh**

# NỘI DUNG

<b>Phần 1: Hệ thống bảo mật thông tin doanh nghiệp .....</b>	<b>7</b>
1. Nhu cầu bảo mật thông tin của doanh nghiệp .....	7
2. Lợi ích của việc áp dụng bảo mật thông tin trong doanh nghiệp .....	7
3. Tiêu chuẩn ISO 27001 là gì ? .....	8
4. ISMS là gì ? .....	8
5. Áp dụng mô hình PDCA để triển khai hệ thống ISMS.....	13
6. Quản lý bảo mật thông tin ISO/IEC 27001:2005 .....	17
6.1. Chính sách an toàn .....	18
6.2. An toàn thông tin trong tổ chức.....	19
6.3. Quản lý tài sản.....	24
6.4. An toàn về nguồn nhân lực.....	27
6.5. An toàn vật lý và môi trường .....	33
6.6. Quản lý trao đổi thông tin và vận hành .....	38
6.7. Kiểm soát truy cập.....	53
6.8. Mua sắm, phát triển và bảo trì hệ thống thông tin .....	65
6.9. Quản lý sự cố an toàn thông tin.....	73
6.10. Quản lý tính liên tục kinh doanh.....	76
6.11. Tuân thủ .....	79
7. Các bước triển khai hệ thống ISMS .....	86

<b>Phần 2 Xây dựng chính sách và quản lý rủi ro IT</b> .....	87
8. Chính sách bảo mật thông tin doanh nghiệp.....	87
8.1 Chính sách bảo mật thông tin doanh nghiệp (EISP) là gì ? .....	87
8.2 Các thành phần liên quan một chính sách.....	88
8.3 Các bước xây dựng chính sách bảo mật thông tin .....	89
8.4 Cấu trúc nội dung chính sách IT.....	93
9. Quản lý rủi ro IT.....	98
9.1 Rủi ro IT là gì ? .....	98
9.2 Phân loại rủi ro .....	99
9.3 Các chiến lược đối phó với rủi ro .....	100
9.4 Quy trình quản lý rủi ro IT .....	101
9.5 Bảng kế hoạch mẫu giúp hỗ trợ việc lập kế hoạch rủi ro IT.....	104
9.6 Xây dựng bản kế hoạch khôi phục hệ thống IT (DRP – Disaster Recovery Plan) ....	106
9.7 Các công việc cần chuẩn bị xây dựng quy trình khôi phục.....	109
10. Phụ lục Template & Ví dụ mẫu đính kèm .....	110
10.1 Quản lý bảo mật thông tin IT .....	110
1. Chính sách bảo mật IT .....	110
2. Đào tạo nhận thức người dùng .....	135
10.2 Quản lý rủi ro IT .....	136
10.2.1. Ma trận phân tích rủi ro IT .....	136
1. Ma trận đánh giá rủi ro IT .....	136

2. Các lỗi thường gặp và cách khắc phục hệ thống IT .....	138
10.2.2. Kế hoạch khôi phục rủi ro hệ thống .....	140
1. Kiểm tra công tác quản lý rủi ro hệ thống IT .....	140
2. Kế hoạch khôi phục hệ thống Server .....	142
3. Kế hoạch khôi phục hệ thống WAN .....	144
4. Thông báo xác nhận đã khôi phục hoàn toàn hệ thống .....	144
5. Thông tin liên lạc cần khi khôi phục hệ thống .....	146
6. Giám sát tiến trình khôi phục hệ thống (I).....	148
7. Giám sát tiến trình khôi phục hệ thống (II).....	150
8. Thông tin cần thiết khi cần khôi phục hệ thống.....	151
9. Hướng dẫn kế hoạch khôi phục rủi ro dữ liệu .....	152
10.2.3. Theo dõi và giám sát sự cố rủi ro xảy ra .....	156
1. Giám sát máy tính trong mạng bị lây nhiễm Virus.....	156
2. Hồ sơ hệ thống ngưng hoạt động.....	157
10.2.4. Báo cáo sự cố rủi ro IT .....	158
1. Báo cáo downtime bất ngờ không theo kế hoạch.....	158
2. Báo cáo sự cố bất ngờ của hệ thống (I) .....	160
3. Báo cáo sự cố bất ngờ của hệ thống (II).....	161
4. Hồ sơ ghi nhận các sự cố của chương trình ứng dụng .....	163
5. Hồ sơ lịch sử khôi phục hệ thống .....	166
10.2.5. Báo cáo sự cố IT theo định kỳ.....	168

1.	Báo cáo trạng thái hệ thống IT định kỳ hàng tuần .....	168
11.	Các tài liệu liên quan khác cần xem .....	171