지란지교에스앤씨

MISO

Management of Information Security Objects

2016년 금융보안감사를 위한 효과적인 대응전략

-지란지교에스앤씨 이성표 과장-

목차

최근 동향

OO뉴스
2015.09.17

금융보안원이 정보보호관리체계(ISMS) 인증 심사를 본격적으로 시작, 이르면 오는 10월 금융보안원 명의의 인증서가 첫 발급될 것으로 전망된다.

ISMS(Information Security Management System)는 조직의 각종 보안위협으로부터 주요 정보자산을 보호하기 위해 정보보호 관리 절차 및 **물리적·기술적·관리적 보호 대책을 체계적으로 수립, 지속적으로 운영·관리하기 위한 종합적인 체계**를 의미한다.

금융보안원 관계자는 17일 "금융보안원이 올해 하반기 진행·진행 예정인 ISMS 심사 대상은 총 26곳"이라며 "이중 첫 번째로 SK증권에 대한 사후 심사를 9월초 진행했고, 후속조치 등이 이뤄진 10월 또는 11월 중 인증서가 발급될 것"이라고 밝혔다.

<중략>

금융기업 중 ISMS 인증 의무대상은 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에서 연간 매출·사용 횟수 등에 따라 규정하고 있다.

금융보안원은 내년까지 세부 통제 항목을 다듬어 보다 금융회사에 적합한 ISMS 심사를 할 계획이다.

금융보안원 관계자는 "금융보안원이 금융권의 IT 환경, 보안 환경 등에서 전문성을 살리기 위해 세부 통제 항목 253개를 금융권에 특화될 수 있도록 내년까지 수정할 방침"이라며 "세부 통제 항목이 금융권에 적합하도록 수정되면 금융 분야의 정보보호 역량이 강화될 것"이라고 설명했다.

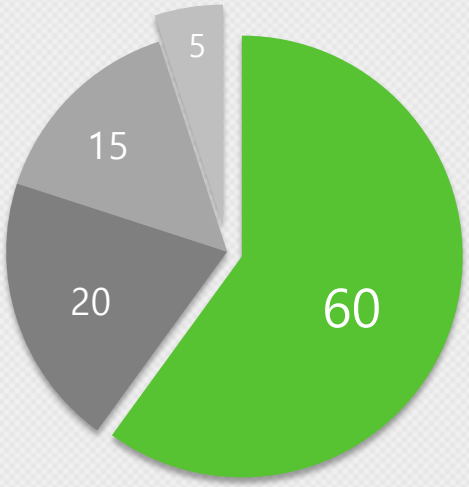
ISMS 심사는 미래부에서 지정한 '정보보호관리체계 인증 등에 관한 고시'에 나와 있는 104개의 기준과 그 하위항목으로 세부 통제 항목이 253개가 있다. 고시는 인증기관 임의로 수정이 불가능하나, 세부 통제 항목은 인증기관에서 수정할 수 있는 권한이 있다.

보안 컴플라이언스 (인증)운영의 어려움

1. 인증 후 운영의 어려움

<컨설팅 후 운영의 어려움>

- 보안규정이 증가하지만 업무는 비슷한 것이 많아 혼란스럽다
- 인력이 부족하여 업무과부화가 발생한다
- 수동으로 하다 보니 업무누락이 되고 증적 유실도 많다
- 보안규정업무를 어떻게 해야하는지 가이드가 필요하다
- 담당자들이 제대로 수행하고 있는지 잘 모르겠다
- 규정에 맞게 업무증적이 잘 관리되는지 알 수 없다



운영의 어려움 통계

1. 인력부족
2. 수동관리
3. 전문성 부족
4. 기타

* 인증의무대상 40여 업체 대상 조사

보안 컴플라이언스 (인증)운영의 어려움

2. 해결 방안 분석

정보보호 관리의 한계점과 개선방안에 관한 연구
.....<중략>.....

3. 공공기관 정보보호 관리체계 개선 제안
.....<중략>.....실시간 정보보호 관리체계 구축을 위해 필요한 요소로는 첫째, 자동화된 데이터 수집이 필요하다. 정보보호 관리체계에서 요구하는 지속적인 관리를 보증하기 위해 자동화된 데이터 수집과 이를 계량화하여 표출해 줄 수 있는 데시보드는 필수적이다.
둘째,정보보호 관리체계의 표준운영 방법인 <계획 → 구현 →점검 → 개선>의 4단계를 유기적으로 지원해 줄 수 있는 관리시스템이 필요하다.
마지막으로 정보보호 관리체계의 평가 항목을 관리해 주고, 실제 수집된 데이터를 계량화 할 수 있는 분석 시스템이
필요하다.....<중략>....

* 논문'정보보호 관리의 한계점과 개선방안에 관한 연구' 발췌

해결방안

지속적인 데이터 수집과
수치화된 데시보드

PDCA 프로세스를 지원하는
유기적인 업무 플랫폼

평가 항목을 관리하고 현황을
수치화하는 기능

평가항목 관리, 업무프로세스 관리, 데시보드를 통해 보안업무현황을 관리해주는 MISO가 해답!

시스템 필요성

1. 시스템 필요성

전자결재 주요 특징

보조활동
- 담당자별 업무분장
- 이행여부 확인
- 진척율 관리
- 증적 관리

본원적 활동
범위 설정 | 조직 구성 | 위험 관리 | 보호 대책 구현 | 사후 관리

정보보호 성과

가치사슬

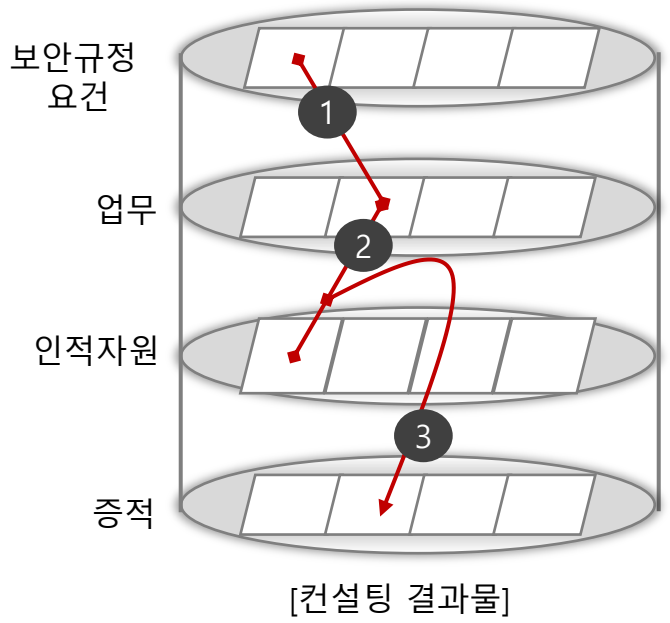
부가가치의 창출
부가가치를 직접 생산하는 본원적 활동과 본원적 활동을 지원해주는 보조활동을 통해 부가가치가 창출됨

가치사슬의 경쟁력
가치사슬의 '약한 고리' 부분이 전체 사슬의 경쟁력 약화 초래

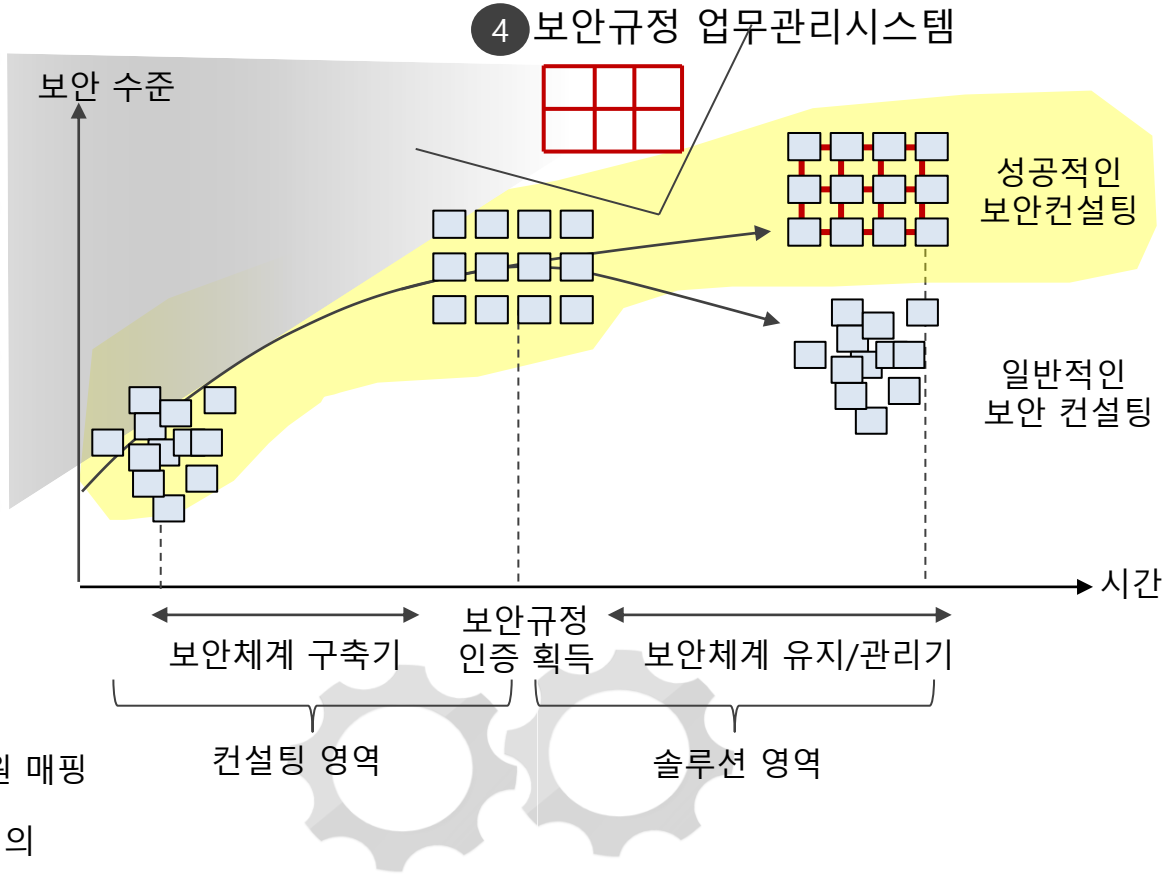
개인정보/ISMS 인증심사 영역	• 인증심사의 주 초점은 본원적 활동영역
컨설팅의 한계	• 인증 획득이라는 형식요소에 초점 인증 이후의 운영방안 제시 미흡 • 일시적인 boom up 이후 지속적인 효과 반감기
문제의 원인	• 관리체계의 수립은 '본원적 활동' 영역인 반면, 수립된 관리체계의 운영은'보조활동' 영역 • 보조활동은 100여 개 이상의 업무의 이행을 관리해야 하기 때문에 노동집약적인 특성, 이로 인한 지속 관리의 어려움 발생 • 즉, 정보보호 활동 가치사슬의 약한 고리는 '보조활동'
해결방향	• 보조활동 영역의 다수 보안업무를 효율적으로 관리하기 위한 중앙 집중화된 업무관리시스템 필요

시스템 필요성

1. 시스템 필요성



[컨설팅 결과물]



1. 보안규정 요건과 관련된 업무 식별
2. 업무를 실제 수행하고 관리해야할 인적자원 매핑
3. 요건에 따른 업무수행의 정형화 및 증적 정의
4. 이전 단계에서 정의된 내용을 보안규정 업무관리시스템을 통해 시스템적으로 자동관리하여 정보보호 관리체계의 영속성 강화

시스템 필요성

2. MISO 소개

MISO Management of Information Security Objects

지속적인 보안업무 가이드로 보안업무 생활화 확립

다양한 구축 경험을 통해 규정의 확대 및 관리, 그룹사 확대 운영, 다양한 업무수행 알림, 기간계 시스템 연동이 가능하도록 설계되었습니다.

표준화된 개발환경	- 전자정부 프레임워크 - Multi DB, OS, WAS, Language - HTML5 - WebService
유연한 사용환경	- 그룹사 기반 운영 환경 - 각종 복수규정 및 내규관리 - 보안업무의 유연한 승인 프로세스 설정
차별화된 서비스	- 지속적인 S/W Upgrade 제공 - 선진화된 방법론으로 최고의 프로젝트 및 유지보수 서비스제공

MISO 주요기능

통계 관리

-월별 업무분포
-분야별 업무분포
-담당자 업무분장현황
-자산위험 관리 현황
-업무진행 현황
-기관 및 부서별 보안수준 현황

통계 규정

-보안규정 추가,수정
-기관별 규정선택 및 항목관리
-규정변경 이력관리
-정책,지침,절차 관리

업무수행관리

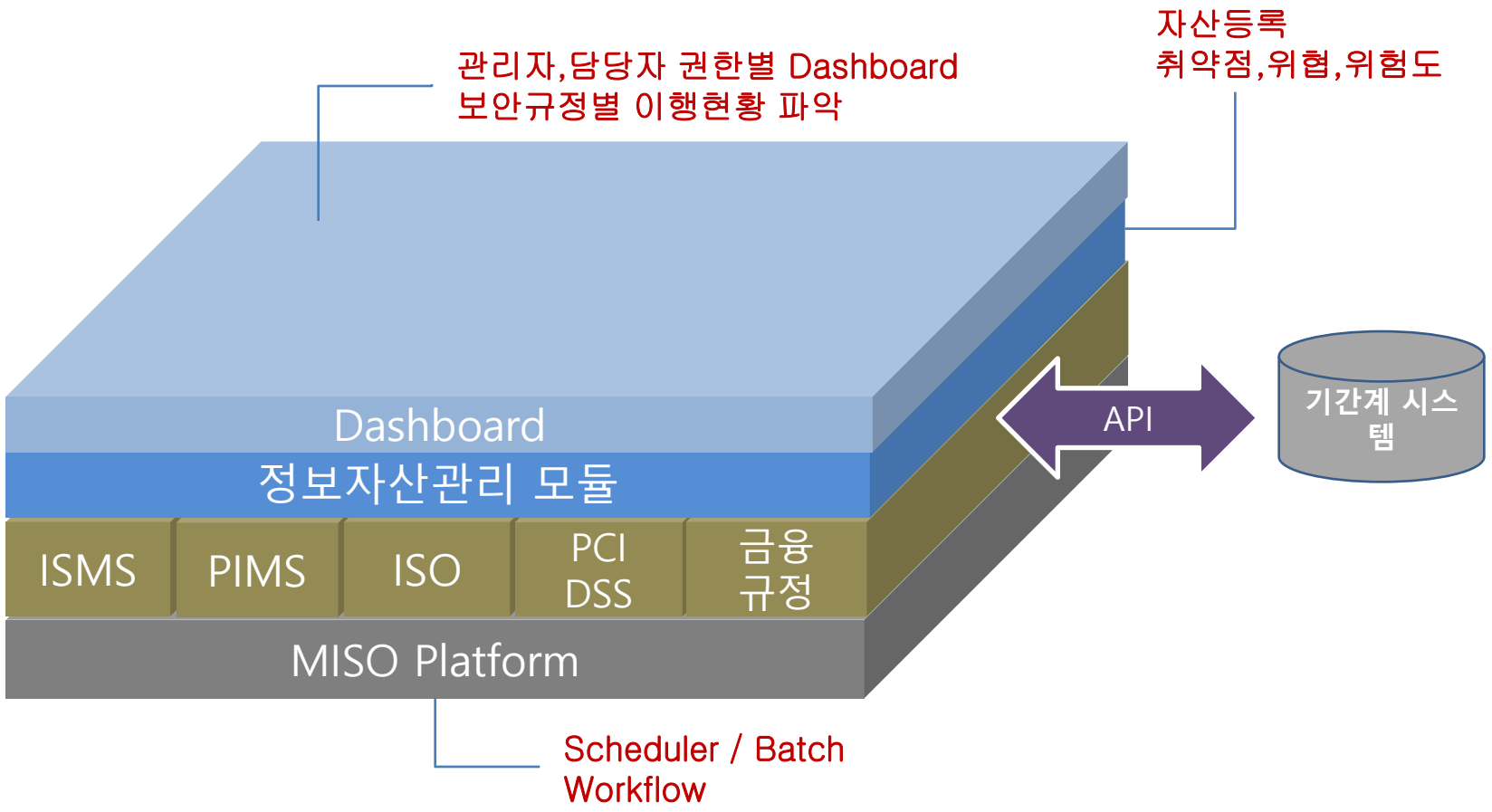
-업무양식 관리
-업무별 규정항목 매핑관리
-업무배치,업무지시
-이행증적 관리

자산관리(옵션)

-자산기본정보 관리
-자산별 연관 보안업무 현황 관리
-보안점검관리
-위험관리
(위험문석,위험평가
위험조치)

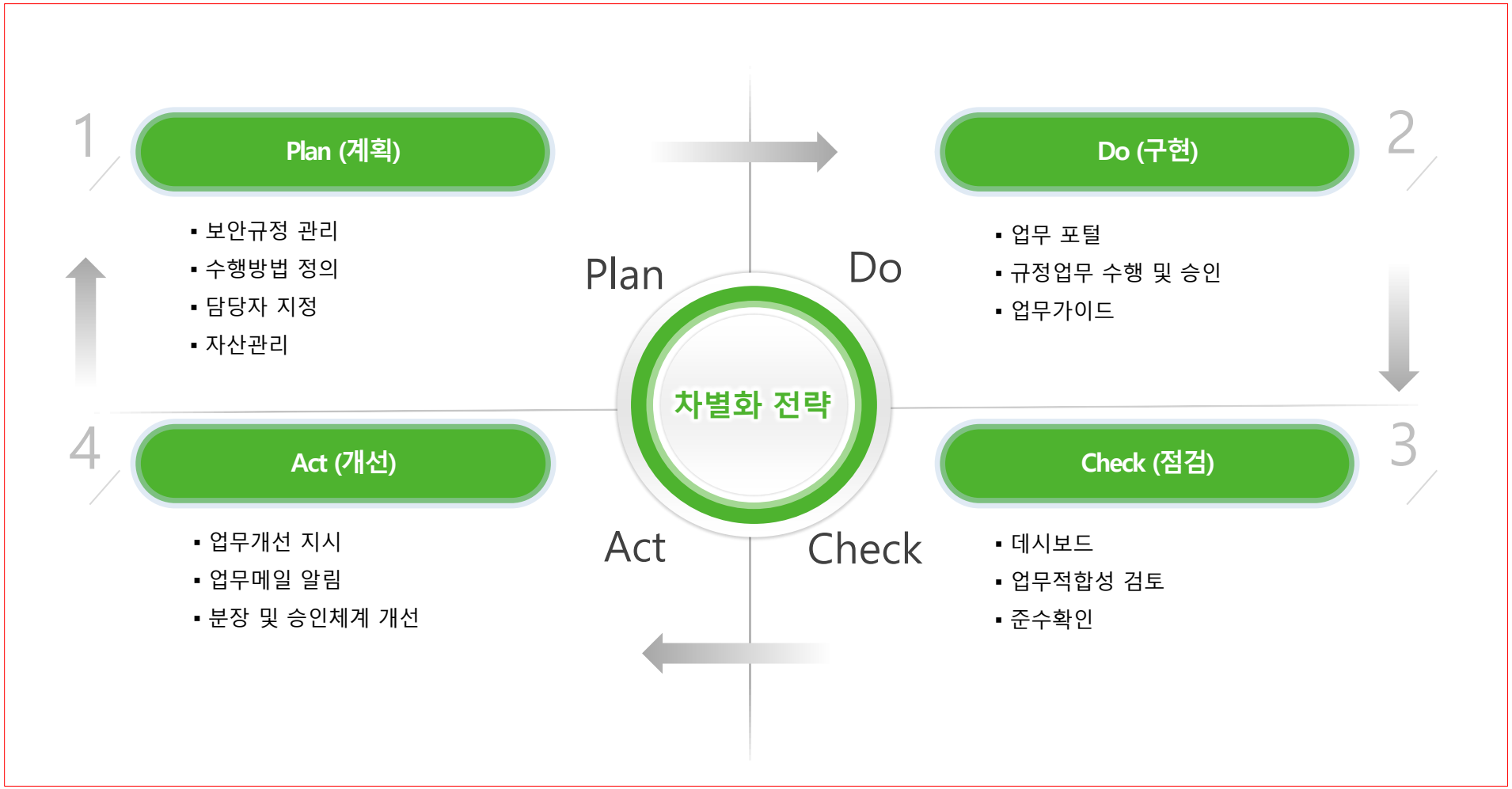
시스템 필요성

3. MISO Platform



시스템 필요성

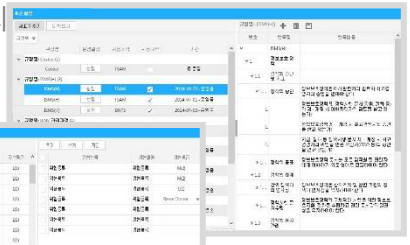
4. MISO 소개 > PDCA 프로세스



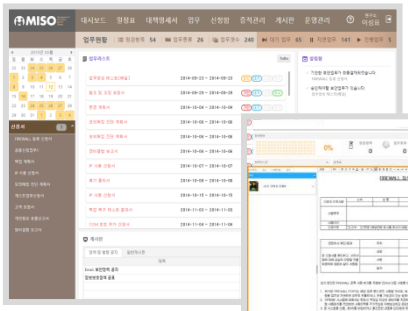
시스템 필요성

5. MISO 소개 > 주요화면

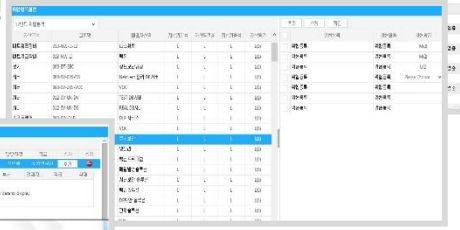
보안규정 관리



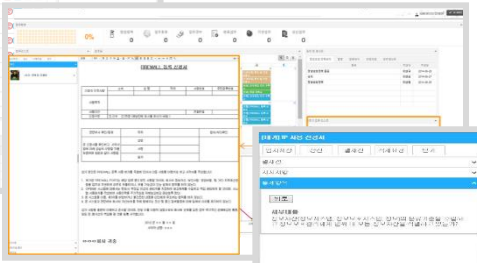
업무 포털



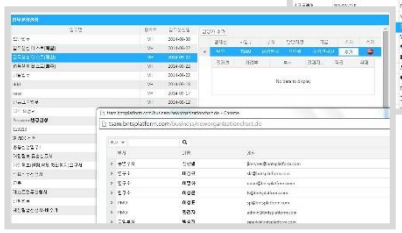
담당자 지정



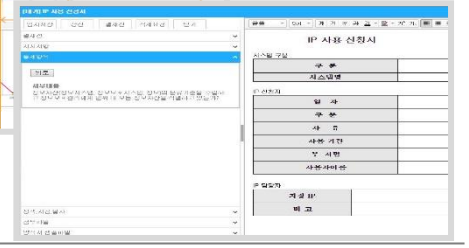
규정업무 수행



자산관리



업무가이드



PLAN

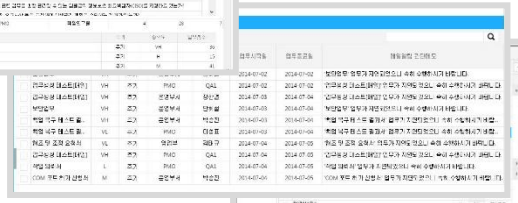
DO

ACT

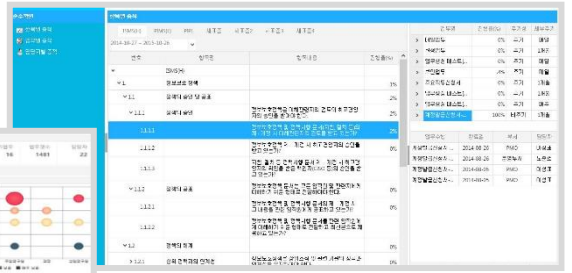
CHECK

분장 및 승인체계 개선

업무메일 알림



업무개선 지시



준수확인

데시보드

시스템 필요성

6. MISO 소개 > 자산위험관리

일반적으로 위험분석 및 평가 수행 시, 자산(Asset), 위협(Threat), 취약성(Vulnerability)의 세가지 요소를 고려하여 위험도(Risk) 산출 및 위험도에 따른 보호대책을 적용합니다.

위험관리 업무 체계

자산관리

자산분석

위험평가

기대 효과

IV

1. 시스템 운영 기대효과(계속)

도입 전

1) 보안담당자의 부족

2) 과중한 보안업무
   : 모든 작업이 수작업

3) 페이퍼 증적(evidence) 관리
   : 분실, 조작의 위험

4) 인증만을 위한 인증 업무
   : 사후관리 문제 발생

5) 보이지 않는 업무체계

보안체계가 무너지게 되는 어려운 현실.

도입 후

1) 손쉬운 체계 유지
   : 담당자들에게 쉽게 사용 가이드

2) 전산화로 업무부하 최소화
   : 증적(evidence), to do 리스트 제공

3) 자산의 위험요소까지 관리

4) 인증체계를 지속적으로 관리
   : 솔루션을 통한 자연스러운 사후관리

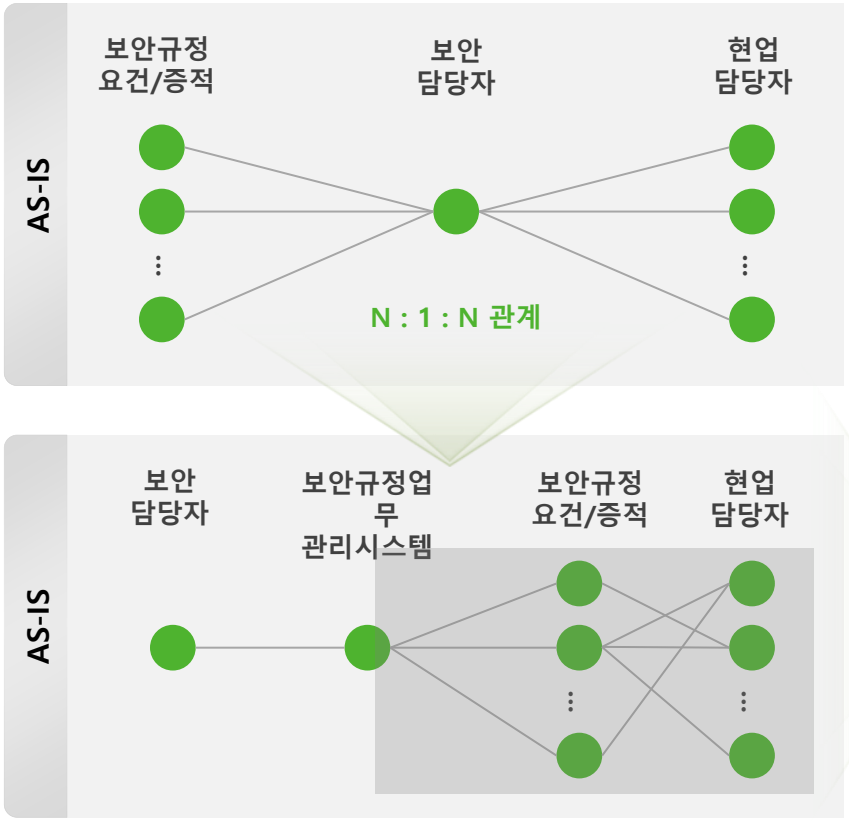
5) 가시적인 업무체계 수립

정보보호에 대한 깊은 이해가 없는 인력도 정보보호업무를 수행할 수 있어야 함.

기대 효과

1. 시스템 운영 기대효과(계속)

업무링크의 변화



보안규정 업무관리 시스템 도입 편익

보안담당자 업무 부하 경감

복잡한 업무 링크 관계를 ISMS증적관리시스템을 통해 간소화 하여 담당자의 업무 부하 경감

보안규정 업무관리 효율성 증대

보안규정 업무관리시스템 기반의 중앙 집중 관리를 통한 업무 효율성 증대

차기 보안규정 인증 비용 절감

체계적인 업무증적 생산/관리를 통해 차기 보안규정 인증 컨설팅(갱신심사) 비용의 획기적인 절감

기대 효과

IV

1. 시스템 운영 기대효과

업무운영의 전산화로 업무시간 50%이상 감소, 전자문서관리로 70%이상 종이 증적 감소.

2~3개월 소모되는 사후심사준비를. 이행증적의 체계적인 관리로 심사준비기간 2~3주로 단축.

주기적인 업무의 자동업무 가이드 및 미수행 업무의 관리로 업무수행률의 향상.

참고자료

1. 인증제도 개관 > 제도 개요 (ISMS)

정보보호관리체계 (ISMS) 정의		조직의 주요 정보자산을 보호하기 위해 정보보호관리 절차와 과정을 체계적으로 수립하여 지속적으로 관리·운영하기 위한 종합적인 체계
개인정보보호 정의		개인정보 보호 관리체계의 수립.운영, 개인정보 처리단계별 기준.절차의 준수 및 안전한 관리, 정보주체의 권리보장 등을 지속적으로 수행하는 일련의 조치와 활동
인증제도 내용	인증 의미	신청기관의 정보보호 혹은 개인정보 보호를 위한 일련의 조치와 활동이 인증심사기준에 부합하고 있음을 승인해 주는 것
	시행 근거	• ISMS: 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조 (정보보호 관리체계의 인증) • PIMS/PIPL: 개인정보보호법률 제133조 (자율규제의 촉진 및 지원)
	대상자	• ISMS: 정보통신망서비스 제공자(ISP), 집적정보통신시설 사업자(IDC), 주요 정보통신서비스 제공자 • PIMS/PIPL: 개인정보 처리자 (업무를 목적으로 개인정보를 처리하는 조직 및 단체)
	벌칙	• ISMS: 정보통신망법 제76조(과태료) …중략… 1천만원 이하의 과태료 부과 • PIMS/PIPL: 없음

참고자료

2. 인증제도 개관 > 인증 기준 (ISMS)

관리과정

	관리과정	항목	세부관리과정	항목 수
1	정보보호 정책수립 및 범위설정	1.1	정보보호정책의 수립	2
		1.2	범위설정	
2	경영진 책임 및 조직 구성	2.1	경영진 참여	2
		2.2	정보보호 조직 구성 및 자원 할당	
3	위험관리	3.1	위험관리 방법 및 계획 수립	3
		3.2	위험식별 및 평가	
		3.3	정보보호대책 선정 및 이행계획 수립	
4	정보보호대책 구현	4.1	정보보호대책의 효과적 구현	2
		4.2	내부 공유 및 교육	
5	사후관리	5.1	법적요구사항 준수검토	3
		5.2	정보보호 관리체계운영현황관리	
		5.3	내부감사	
계				12

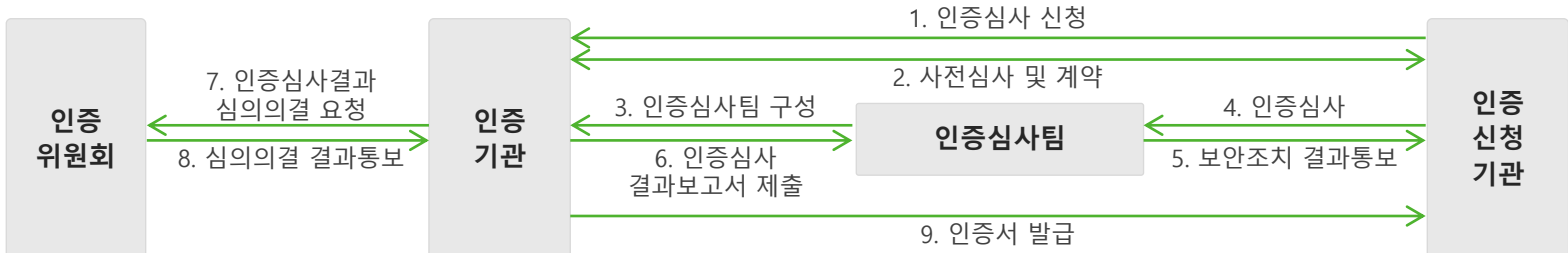
정보보호대책수립

단계	통제분야	통제목적	항목 수
1	정보보호정책	정책의 승인, 공표, 유지관리 등	6
2	정보보호조직	조직 체계, 책임과 역할	4
3	외부자 보안	외부자 보안 이행	3
4	정보자산분류	정보자산 식별, 분류, 관리 등	3
5	정보보호교육	계획 수립, 시행 및 평가	4
6	인적보안	정보보호책임, 인사규정	5
7	물리적보안	물리적보호구역, 사무실보호 등	9
8	시스템개발보안	분석, 설계, 구현, 이관보안 등	10
9	암호통제	암호정책, 키관리	2
10	접근통제	정책, 권한관리, 인증 및 식별 등	14
11	운영보안	시스템 및 서비스 운영 보안 등	22
12	침해사고관리	절차 및 체계, 대응 및 복구 등	7
13	IT재해복구	체계 구축, 대책 구현 등	3
계			92

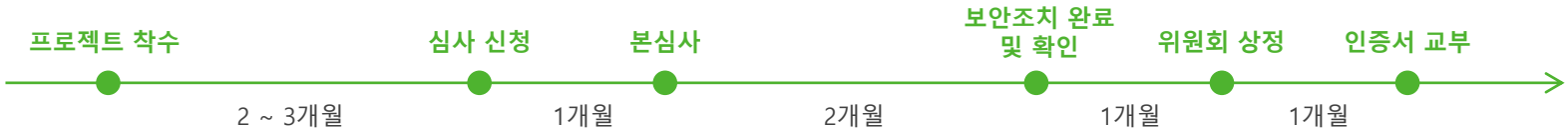
참고자료

3. 인증제도 개관 > 인증절차 및 유효기간

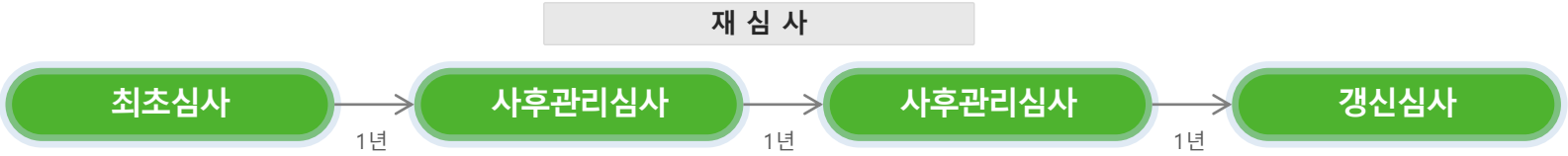
인증 절차



인증 소요 기간



인증 유효 기간



- 최초심사: 정보보호관리체계 인증 취득을 위한 심사
- 재심사: 인증을 받은 정보보호관리체계의 범위 내에서 중대한 변경이 발생한 경우의 심사
- 사후관리심사: 정보보호관리체계를 지속적으로 유지하고 있는지에 대한 심사(연 1회 이상)
- 갱신심사: 유효기간(3년) 만료인 이전에 유효기간의 연장을 목적으로 하는 심사

참고자료

4. Architecture of information security management system

Security Equipment
N/W Equipment
Server
PC
Security Policy
Security Manager

Collecter / Analyzer

Collector

Collected Information
Firewall Log
IDS/IPS Log
Vaccine Log
WAF Log
Web Log
Resource Info.
Account Info.
Network Log
Port Info.
Security Policy Document
Policy / Standard
Security Work Result
Security Manager / Division
Security Manager

Analyzer

Real-Time Analysis
Periodic Analysis
Context Analysis
Web Page Monitoring
Hacking Symptoms Analysis

Security Assurance Manager

Real-Time Management

Configure Management

Security Control Manager	Analysis Method Manager	Police Manager
Collection Policy Manager	Security Work Manager	Event Manager

DashBoard

Viewer / Reporter

Security Level Quantification
Intuitive level management
Security Investment ROI
Measuring security
problem checking

Compliance establishment
(I는 certificate, etc.)
Business convenience
improvement

Security accident
Prevention
Cause of accident
analysis

감사합니다.