

BoB(Best Of the Best) 보안컨설팅 트랙

보안컨설팅 이해 및

BoB 보안컨설팅 인턴쉽 과정소개

2013. 11. 30

김 홍 진/ BoB(Best of the Best) 멘토

발표자 소개...



인적사항

- 이 름 : 김 홍진
- 소속 및 직급 : LG CNS / 차장
- E-Mail : hjkim0892@gmail.com

자 격 증

- 정보관리 기술사(96회), 2012. 5
- PMP, 2005.4
- CISA, 2004.4

강의경력

- 한국정보기술연구원 주최 BoB 멘토링
- 중소기업 역량강화 사업 참여
- 한국생산성 본부 IT기술사 모의고사 출제 및 채점위원
- 한국생산성 본부 IT기술사 합숙과정 멘토링
- LG CNS 사내강사
- 저술 및 강의 활동 수행 중



Table of Contents

1. 컨설팅의 개념 이해

2. 보안 컨설팅 이란?

3. BoB 보안컨설팅 인턴쉽

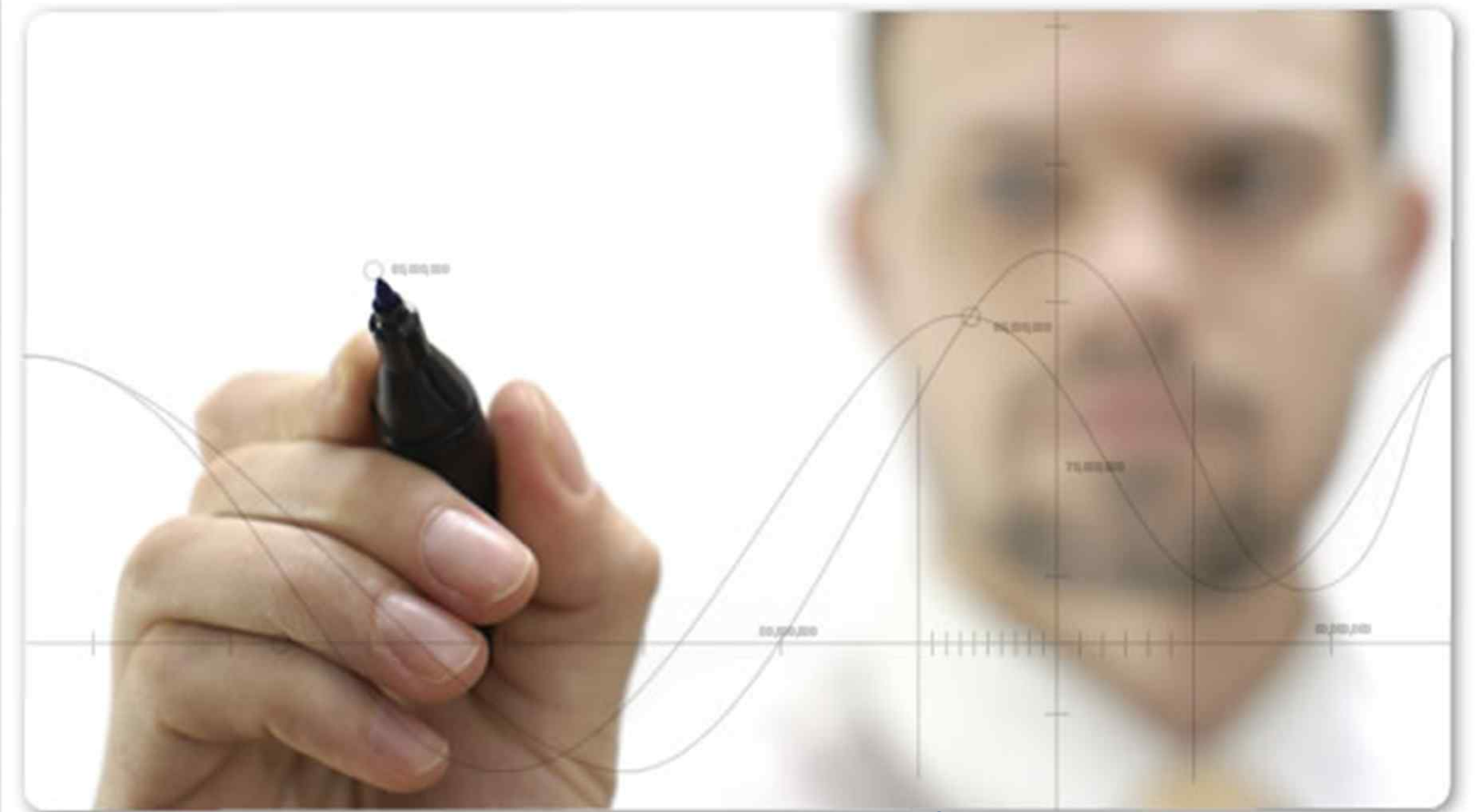




1. 컨설팅의 개념 이해

What is the “CONSULTING” ?

Acting in an advisory capacity on professional matters



- Origin : Collins English 30th Anniversary Edition -

문제해결 전문 외부 서비스

- 기업으로 하여금 당면한 문제들을 분석, 해결할 수 있도록 외부업체에서 도와주는 것.
- 성공/실패 사례를 타기업에 접목시킬 수 있도록 도와주는 전문적인 서비스.

경영자의 목표 지원/ 조언자

- 경영자가 자신의 판단에 따른 합리적 경영추진이 가능 하도록 객관적인 입장 제시
- 경영자가 추구하는 목표를 현실화 할 수 있도록 환경여건을 제시하는 서비스.

문제 해결방안 제시

- 잘 해결되지 않는 문제점을 도출하여 신기술 혹은 새로운 방법으로 해결방안 제시.
- 기존 업무의 틀에서 벗어나 회사를 위해 고민하는 새로운 전기를 마련

Creative Thinking	Logical Thinking	Fact-Based Thinking	컨설팅의 기본역량
Modeling Skill	Research Skill	Problem-Solving Skill	방법론과 툴에 대한 이해
Documentation Skill	Communication Skill	Presentation Skill	효과적인 의사전달

1. 다양한 문제 경험

컨설턴트들은 수년 동안 많은 기업들이 직면한 문제들을 다루어왔을 뿐만 아니라 컨설팅 프로젝트로부터 얻은 경험들을 유용하게 사용하여 새로운 상황에 직면하고 있는 고객기업에게 조언할 수 있도록 학습해왔음



2. 경험과 정보가 풍부

컨설팅회사에 고용된 컨설턴트들은 다른 고객들을 위해 일했던 동료 컨설턴트들의 경험으로부터 많은 것을 간접적으로 학습할 수 있으며, 회사가 축적한 방대한 양의 노하우를 활용할 수도 있음



3. 꾸준한 학습자

컨설턴트들은 새로운 경영이론이나 개념, 방법, 시스템 등의 발전에 뒤처지지 않기 위해 지속적으로 노력하고 있음



자신의 포지셔닝(Positioning)은?

여러분은 어떤 컨설턴트입니까?

- ✓ Certified vs. Qualified

컨설턴트, 과연 그들이 비즈니스를 알까?

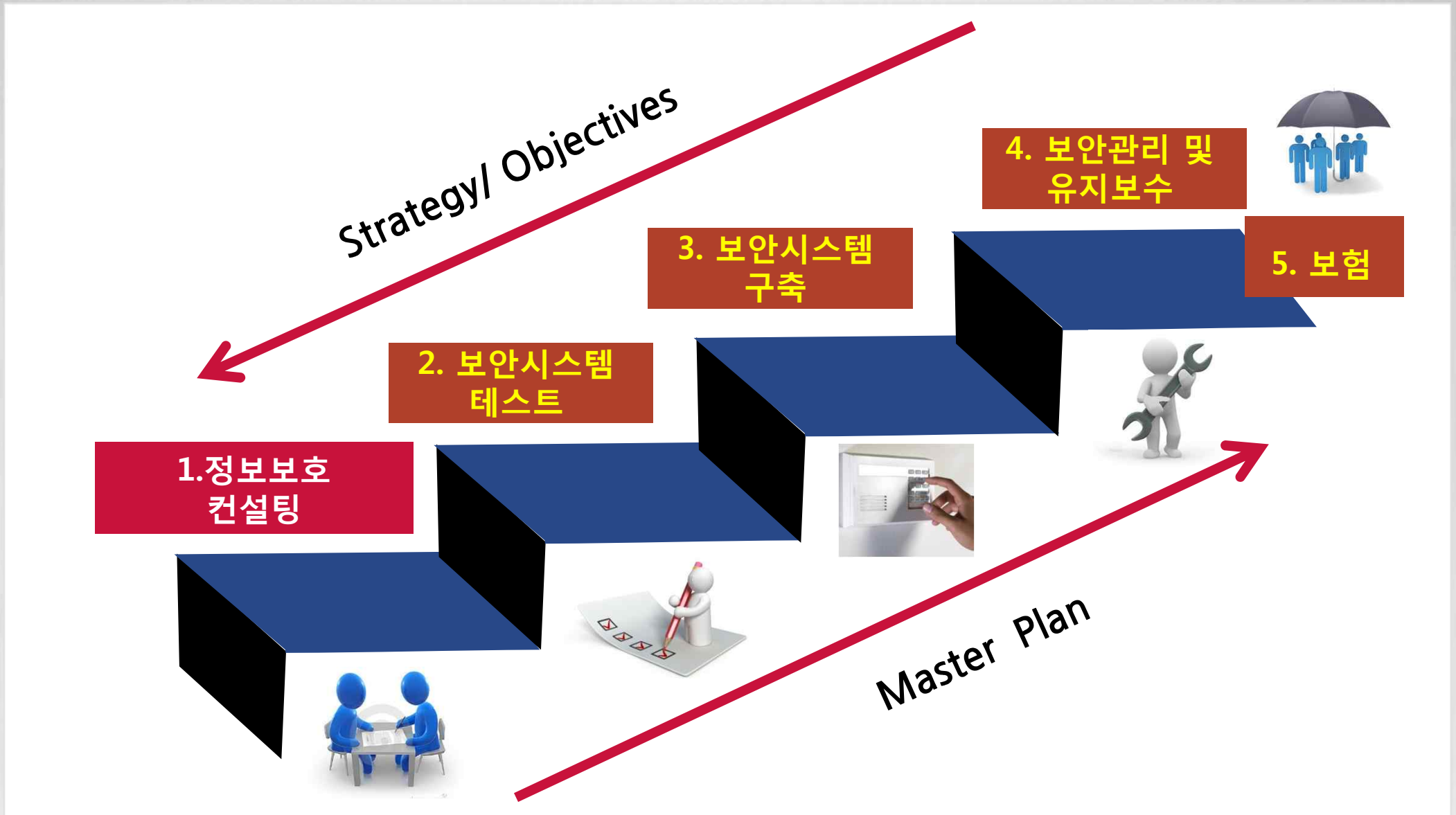
- ✓ 여러분은 어떤 산업의 비즈니스를 알고 있습니까?
 - *ERP 모듈 컨설턴트 vs. 업종 전문가 vs. 프로세스 컨설턴트 vs. 비즈니스 컨설턴트*

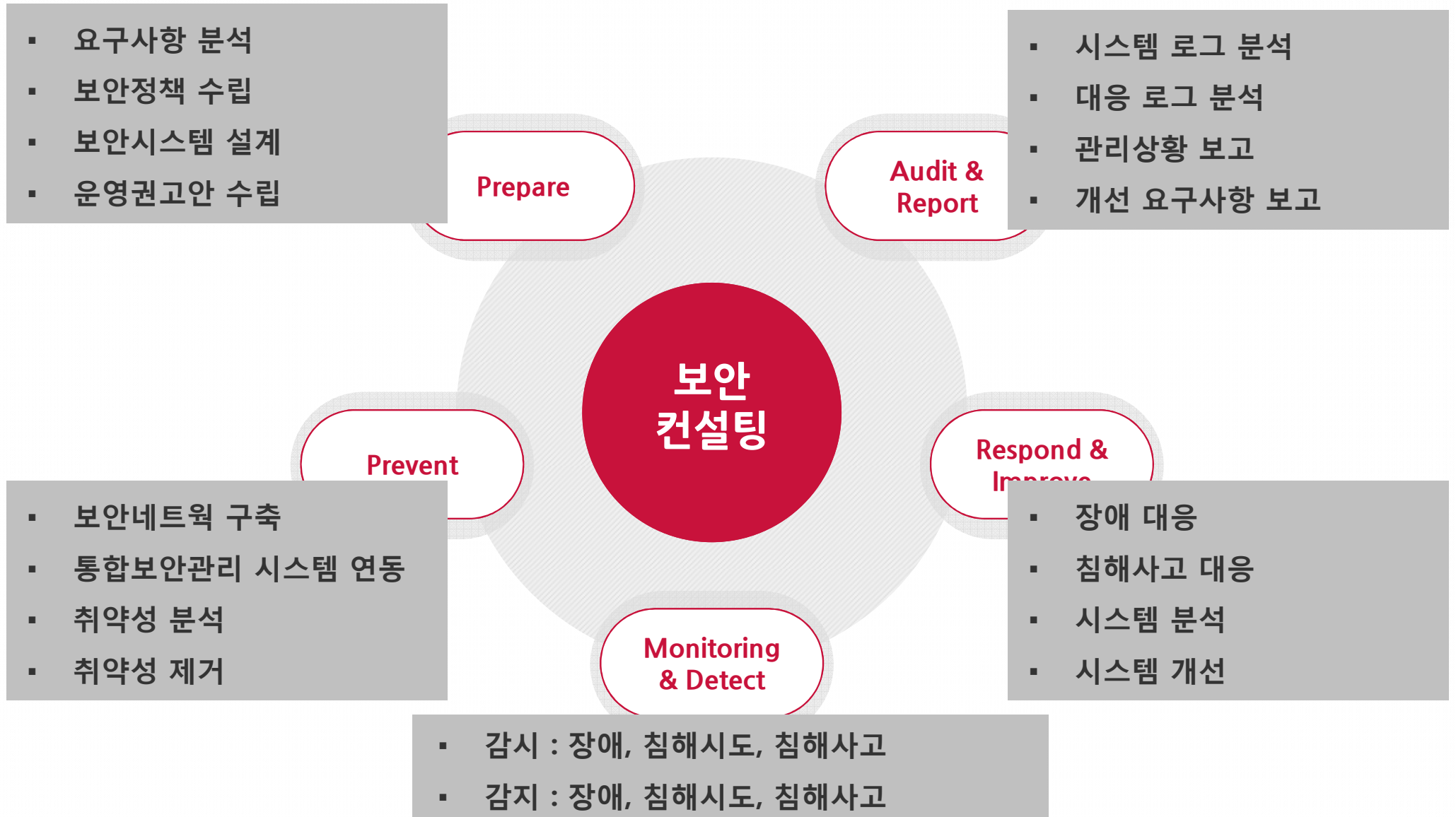
컨설팅 본질은,

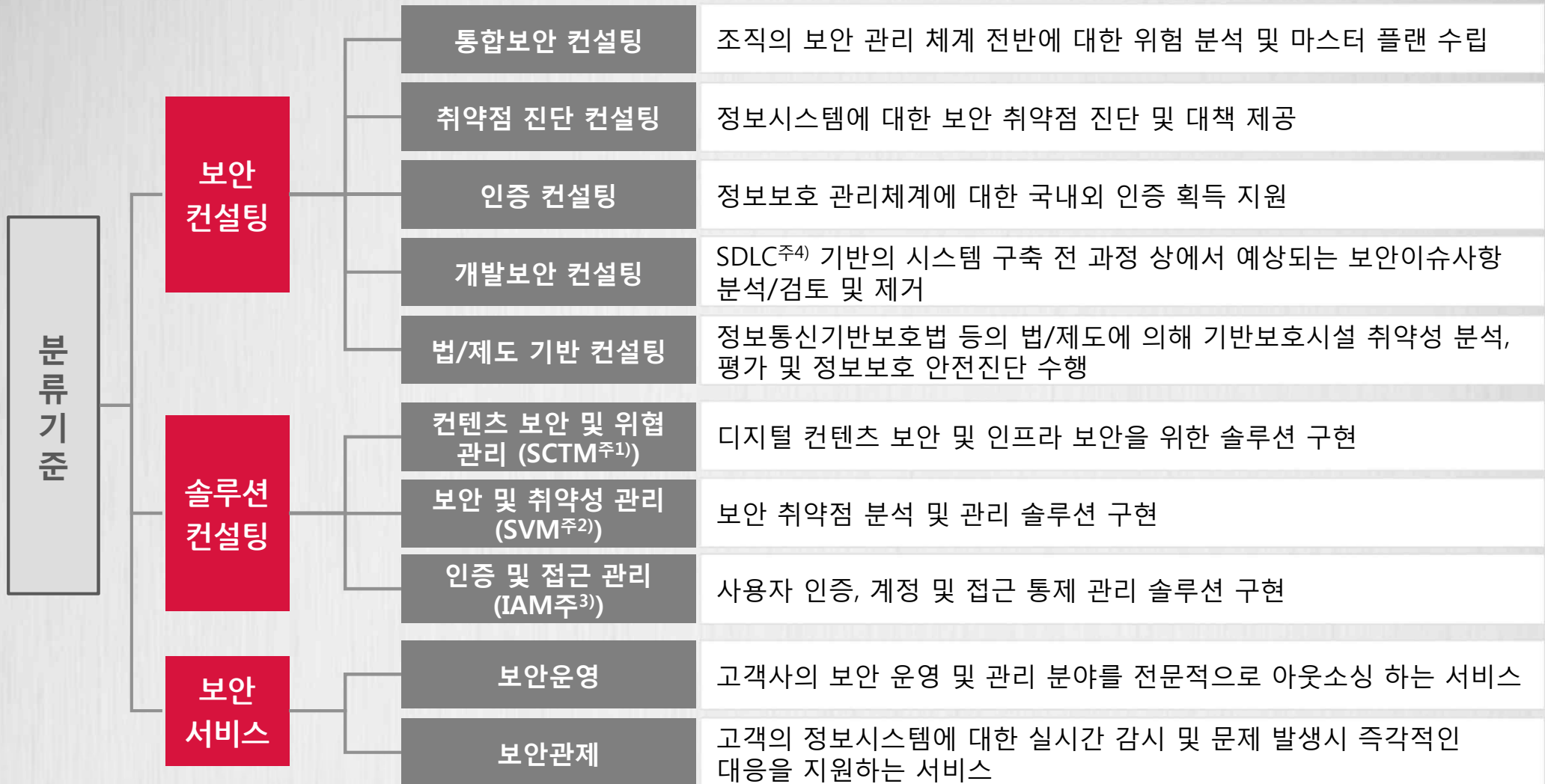
끊임없는 질문과 생각, 패기와 도전정신

2. 보안 컨설팅 이란?









주1) SCTM : Secure Content and Threat Management
주3) IAM : Identity and Access Management

주2) SVM : Security and Vulnerability Management
주4) SDLC : S/W Development Life Cycle

정의	조직의 보안 관리 체계 전반에 대한 위험 분석 및 마스터플랜 수립 컨설팅
주요 기능	주요 정보자산에 대한 관리적/기술적/물리적 취약점을 파악하고 위험분석을 통해 체계적인 보안 마스터플랜을 수립함

제공 서비스	기대효과
<ul style="list-style-type: none"> • 현황 진단 및 위험분석 • 진단 및 분석 결과에 따른 대책 수립 • 조직의 업무 특성에 맞는 보안 정책/지침/절차의 제·개정 및 보안 마스터 플랜 수립 • 취약점 진단 컨설팅 및 정보유출 방지 컨설팅 	<ul style="list-style-type: none"> • 조직의 특성, 실정에 적합한 보안 관리체계 확립 • 중.장기 정보보호 계획 수립 및 이행체계구축 • 임직원들에 대한 보안 인식 제고 • 비즈니스 연속성을 위한 기반 마련

정의	정보시스템에 대한 보안 취약점 진단 및 대책을 제공하는 컨설팅
주요 기능	모의해킹과 함께 대상의 기술적인 진단 및 실증적 해킹 가능성 점검 후 그에 따른 대응책을 수립함

제공 서비스

- 서버/네트워크/DB/PC/어플리케이션 등 모든 정보 시스템에 대한 기술적 침해요소 진단 및 대응방안 수립
- 중요 정보시스템에 대한 기술보안 아키텍처 및 마스터플랜 수립

기대효과

- 주요 정보자산의 위협 및 취약점 제거
- IT인프라에 대한 안정성 확보
- 보안에 대한 경각심 고취
- 보안컨설팅 및 정보보안에 대한 투자유도

정의	정보보호 관리체계에 대한 국내외 인증 획득을 지원하는 컨설팅
주요 기능	정보보호관리체계 국제 표준인 ISO27001 또는 정보통신부의 정보보호관리체계 KISA ISMS 인증 획득을 지원함

제공 서비스	기대효과
<ul style="list-style-type: none"> • 인증 획득을 위한 지원 : 환경/자산분석, 취약점 분석, 위험분석 및 평가, 정보보호 대책 및 계획 수립 • 사후 심사 지원 	<ul style="list-style-type: none"> • 표준화된 정보보안 관리체계 수립 • 공신력 있는 인증 획득을 통한 조직의 이미지 향상 및 고객 신뢰도 증진 • 보안사고 예방 및 피해 최소화 • 정보보호 관리 능력 향상

정의	SDLC 기반의 시스템 구축 전 과정 상에서 예상되는 보안 이슈사항을 분석/검토 및 제거하기 위한 컨설팅
주요 기능	기업 애플리케이션 개발 단계에서부터 계획, 분석, 설계, 구축, 테스트, 운영의 단계마다 보안을 고려하여 발생 가능한 취약점을 분석/제거 및 방안을 제시함으로써 기업 전반의 보안을 강화함

제공 서비스	기대효과
<ul style="list-style-type: none"> • 시스템 구축 단계별 위험 분석 • 보안 요구사항 정의 및 보안기능 설계 • 보안기능 테스트 및 보안성 검토 	<ul style="list-style-type: none"> • 운영 단계에서 발생 가능한 위험의 사전제거를 통해 시스템의 보안성 강화 • 개발 완료 후 보안 시스템 구축에 따른 추가 및 변경 작업 최소화 • 기업 전체의 보안정책과 부합 가능

정의	정보통신기반보호법에 의한 기반보호시설 취약성 분석/평가 컨설팅 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의한 정보보호 안전진단 수행 컨설팅
주요 기능	주요정보통신기반시설 취약점 점검 서비스 : 금융감독위원회/정보통신부 취약점 분석/평가 기준을 반영한 보호대책을 수립함 (연1회)
	정보보호 안전진단 : 관리적/기술적/물리적 보호조치에 대한 세부조치사항 중 대상별로 차별화된 항목 점검을 통해 필증을 부여함 (연1회)

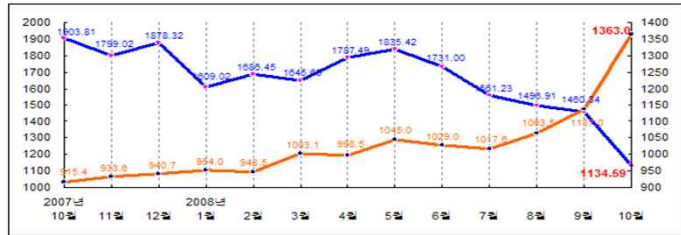
제공 서비스

- 기반시설 취약점 점검:취약점 분석/평가 계획 수립 및 대상 선별, 위험 및 취약요인 분석, 기존의 보호대책 분석 및 취약점 평가, 보호 대책 수립
- 정보보호 안전진단:정보통신 서비스 제공자의 정보보호조치 이행 및 관리적/기술적/물리적분야 진단, 대책수립 및 심사를 통한 필증획득 업무 수행

기대효과

- 법/제도의 준수
- 고객의 안정성 및 신뢰성 확보
- 보안사고 피해 예방

보안현황 및 위험진단



수요기관의 IT환경에 대한 분석을 통해 현황을 파악하고, 자동화 된 Tool을 이용한 취약성 점검을 실시하며 위험을 진단함

개선방안 도출



현황 파악에서 이루어진 결과를 바탕으로 수요기관의 IT환경을 보안의 관점에서 최적화 할 수 있는 개선방안을 도출함

마스터플랜

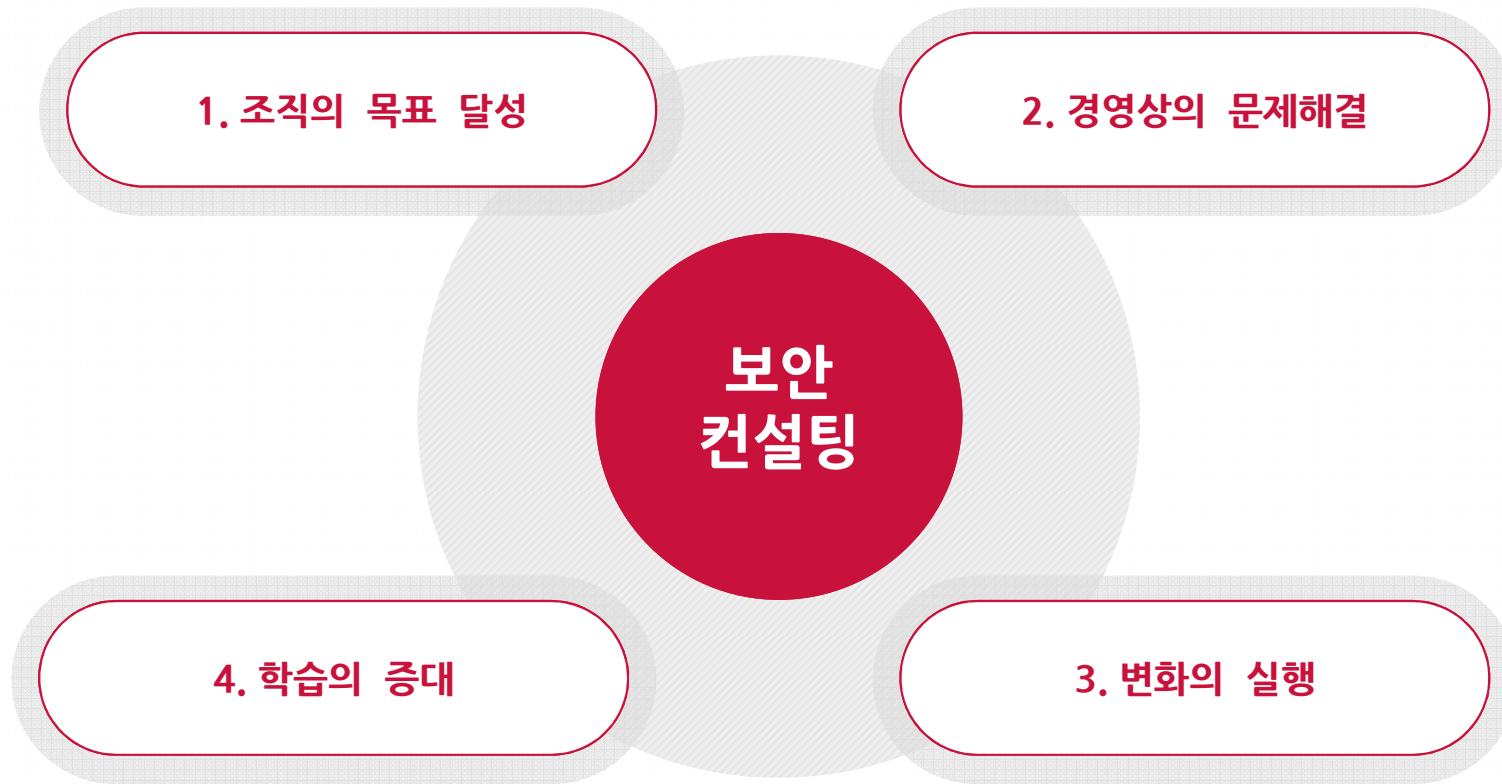


수요기관의 환경에 최적화 된 체계를 일정과 구축비용 등의 제반 사항을 스케줄링에 따라 구체적으로 실행함

시스템 설계



개선방안을 바탕으로 하여 수요기관의 보안성을 향상 시킬 수 있도록 관리/기술/물리적인 관점에서 체계를 설계함.



‘보안컨설팅(Security Consulting)’은 보안업무 추진을 지원하는 자문서비스

1. 기업의 보안수준 제고

- 정보자산에 발생할 수 있는 위험요인 등을 사전에 파악하고 보호대책 수립 가능
- 보안현황 파악하고 문제점 개선시키기 위한 목표를 정의함으로써 보안수준 제고 가능



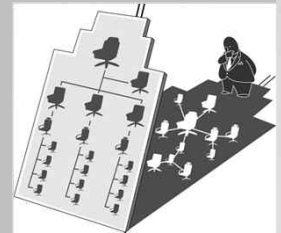
2. 보안 관리체계에 대한 인증획득

- ISMS 및 ISO/IEC 27001 보안 관리체계 기준의 준수 여부를 평가 및 인증 획득 가능
- 국내외 보안 관리체계 인증 획득 시 기업의 대외이미지 향상, 고객신뢰도 향상



3. 기업 내 역학관계 해결

- 보안 관련 문제에 대해 내부직원은 제시할 수 없는 경우가 발생할 수 있음
- 그러나 외부 컨설턴트는 기업 내 역학관계로부터 영향을 덜 받으므로 쉽게 문제 해결



4. 종업원 교육 및 법적 준거성 확보

- 종업원 교육을 실시함으로써 보안업무의 기업내 적용이 원활해질 수 있음
- 보안 관련 법,제도적 장치에 대한 이해를 통해 효과적이고 경제적인 활용 가능해짐



I. 착 수(WHY)

II. 진 단(WHAT)

III. 계획수립(HOW)

IV. 실행 및 종료 (WHEN)

컨설팅 업무

1. 현황 및 환경분석(예비진단)
2. 취약점 분석 및 위험평가
3. 보안 마스터플랜 수립
4. 보안정책 및 지침수립
5. 보안시스템 구축

컨설팅 범위

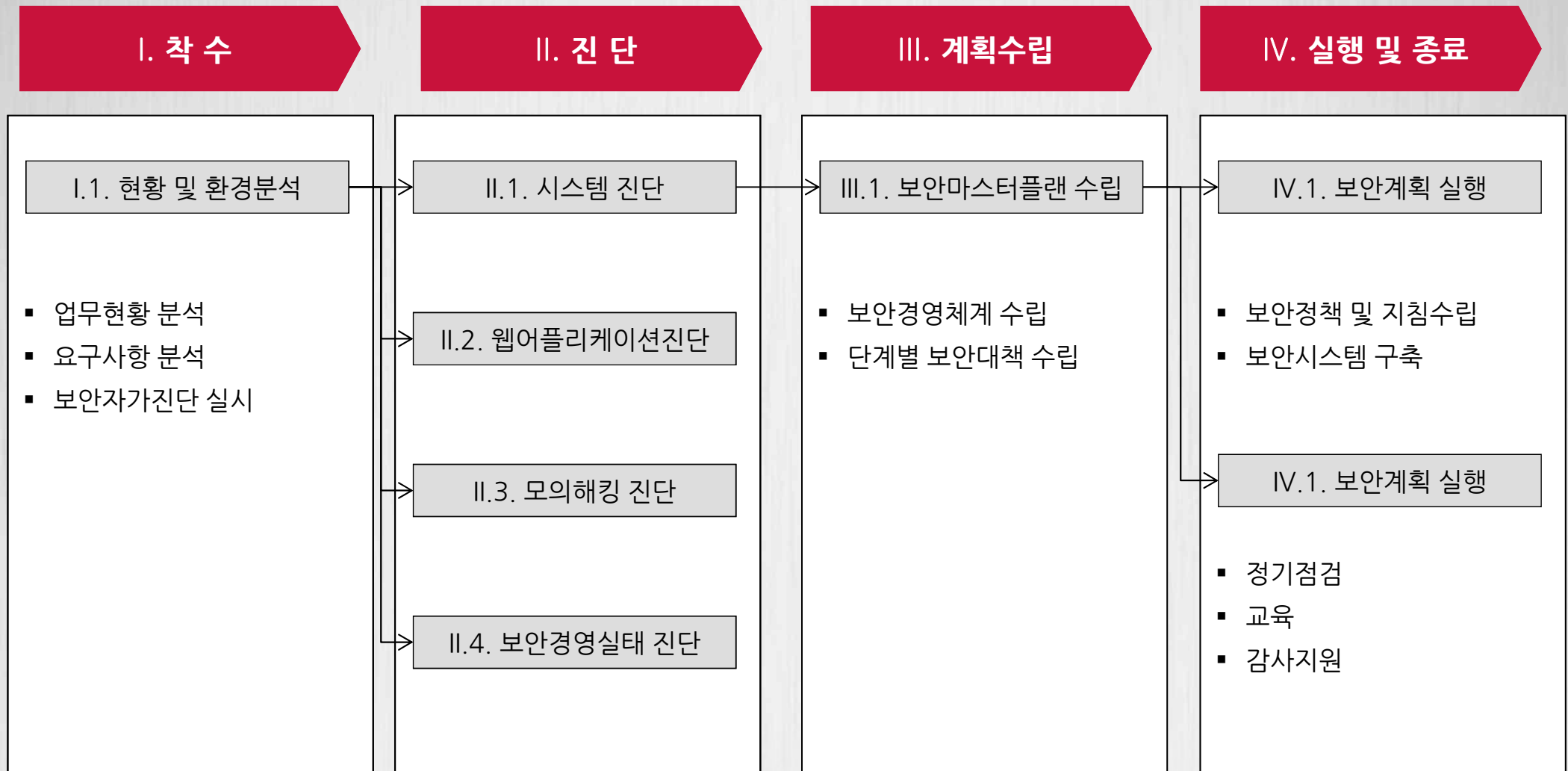
1. 기업의 시스템 현황 분석
2. 관리적, 물리적, 기술적 진단/분석
3. 보안 취약점 대응 시스템 구축방안 수립
4. 보안 정책 및 마스터 플랜
5. 사후 관리 및 교육

보안업무
프로세스 개선

보안정책
및 지침수립

보안
인식제고

보안역량 강화를 위한 마스터플랜 수립 및 솔루션 적용



현황 분석

현재 기업의 상태를 분석하며 SW, HW, NW 등 제반 시스템에 대한 분석을 수행함

취약점 점검

분석된 현황에 대한 주요 취약점 부분을 점검함

이행 과제

파악된 취약점을 분석하여 주요 이행과제를 도출함

진행 계획

이행과제에 대한 사업 계획 및 예산 등 진행계획을 수립함

3. BoB 보안컨설팅 인턴십



'12년 BoB 보안컨설팅 트랙 결과는...



보안컨설팅 부각의 배경

내부 환경 변화

- 정보보호 측면에서 중장기적인 고객의 발전 방향성 정립 필요
- 정보보호 전담조직의 정보보호 선도적 역할 수행 요구 증대
- 기업의 정보보호 수준 향상 및 지속적인 유지관리 필요

외부 환경 변화

- IT와 물리 보안 영역의 정보보호 수준 격차로 인한 핵심 기업정보 유출사고 사례 급증
- 해킹에 의한 개인정보 대량 유출
 - 대규모 포털사이트 해킹을 통해 회원개인정보 대량 유출

보안컨설팅의 목적

통합관점의 마스터플랜 수립

정보보호 전담 조직 역량 강화

지속적 보안수준 향상 방안 수립

정보보호 마스터플랜 수립

- 보안 정책/지침 등의 정보보호 규정 체계

물리적/관리적 영역

- 외곽보안, 출입보안, 내부보안 등 물리적/관리적 보안 대응체계

취약점 진단 및 모의해킹

- 시스템 자산의 실질적인 보안 취약점 파악 및 대응책 마련

개인정보 보호

- 사용자 개인정보 및 내부정보 보호 및 영향평가

정보보안 컨설팅

보안정책

- 국내외 IT Compliance에 따른 보안규정 및 정책

컨설팅 역량 확보

사례기반의 보안기술

보안 취약점 분석 기법 습득 및 컨설팅 역량 확보

BoB 보안컨설팅 트랙 개요

1. 기업 IT자원에 대한 현황분석
2. 응용 Application 취약점 분석 기법
3. 물리적/관리적 보안 취약점 분석 및 대응방안 제시
4. 컨설팅 역량 확보를 위한 Consultancy 확보방안 마련
5. 보안컨설팅 산출물 작성 및 사례 연구

멘토링 수행 방법

- 강의 / 멘토링 진행
 - 과제 관련 강의 진행
 - 오프라인 멘토링 진행
- BoB 페이스북 또는 카페를 통한 온라인 멘토링 수시 진행

강의주제	강의내용
개인정보보호 실무	개인정보 보호 법적규제/ 개인정보 보안의 중요성/개인정보 영향평가(PIMS)
정보보호 성과관리	정보보호 정책의 전반적인 과정을 이해/ 성과 관리기법 학습
컨설팅이란 무엇인가?	컨설팅의개요 / 컨설팅의유형 / 컨설턴트로서의자질
프로젝트 방법론	프로젝트의개요 / 방법론의구성요소 / 방법론의유형
컨설팅 실무사례 및 컨설턴트 직무	기업에서바라는인재상 / 컨설턴트의기업에서역할 / 직업으로서의컨설턴트
Documentation 기법	컨설턴트로서의올바른Documentation 기법학습 / 효과적인 Communication 기법
컨설팅 방법론	-컨설팅프로세스이해 / 절차별 컨설팅절차 이해 및 산출물이해
고객 설득적 Presentation기법	컨설팅의최종산출물에대한효과적전달 기법요구/ 효과적인산출물작성기법
보안관련 표준 및 정책	-ITCompliance관점의주요보안관련법규및정책이해/ ISO27001/ISMS/CA
Big Data, SNS의 보안	SNS등의 최신 Trend 기반 보안 이슈
무선시스템 기반의 보안취약점	무선네트워크환경의이해/ 무선네트워크기반의보안취약점분석
관리적 관점의 보안 컨설팅 방향	관리적 관점의 보안 요소에 대한 세부요소 이론 이해
IT융합환경에서의보안취약점	IT융합환경의이해 /융합환경에서의보안취약점

보안컨설팅 멘토링 특징

- **보안정책 및 컨설팅 분야 학계/ 산업계 전문가 멘토링 체계**
 - 국내 최고 보안 관련 학계 정보 보안 전문가
 - IT기술사 자격 보유 멘토 참여
 - 전문 지식과 경험 기반 멘토링
- **현장경험 기반의 프로젝트 운영**
 - 국내 다양한 프로젝트 경험 기반 운영
 - 현장경험 Lessons Learned 제공
- **인생 조연자 역할의 멘토링 수행**
 - 사회진출에 필요한 다양한 정보 제공
 - 학습과 인생의 Mentoring Balance 수행

보안 컨설팅 멘토링 기대효과

- 보안정책에 대한 체계적인 학습
- 개인정보 보호 및 개인정보 영향평가 심화학습
- 전문 컨설팅 기법 습득 및 실습을 통한 Consulting Competency 확보
- 보안관련 주요 기술의 이해 및 습득
- 기업 보안 취약점 분석 기법 및 Tool 활용능력 향상
- 기업 모의해킹 기법 및 주요 사례 습득
- 컨설팅 수행을 위한 Presentation 및 Documentation 역량 확보
- 사회 진출 및 인생에 대한 다양한 경험 습득
- 실무중심의 다양한 현장 사례 습득

현장형 보안 컨설팅 전문 인재양성을 위한 가상 보안컨설팅 인턴십 시나리오 개발

보안사고에 능동적인
대응 구현

전문 지식을 보유한
화이트 해커 양성

국가 안보 대응 및 정보 보안
산업 역량 강화

보안 사고의 지속적인 증가

- 최근 급증하는 해킹 및 침해 사고에 대한 능동적인 대처가 부족
- 보안에 대한 인식 부족으로 인해 국가적 규모의 침해 사고의 증가
- 보안침해, 공격기법 진화에 대응 능력 부족

보안 전문 인력의 부족

- 보안침해에 대응할 수 있는 보안 인력의 부족으로 국가 및 기업의 침해 증가
- 전문 보안인력 부족에 따른 국가적 차원의 인력 양성 체계 마련 시급
- 경력위주 탈피, 체계적 신규 보안전문인력 양성 커리큘럼 구현 미흡

1

보안컨설팅 인턴십 수행에 대한 사전 지식 습득

- 문서작성 및 PT역량강화 교육 커리큘럼 구현
- 보안컨설팅에 부합하는 프리젠테이션 경진대회 개최
- BOB 멘토링교육 및 보안기업 컨설턴트의 진로지도 제공



2

보안 컨설팅 인턴십 현장실습 수행

- 실전과 동일한 보안컨설팅 프로젝트 수행
- 보안 컨설팅 실습에 적합한 다양한 업종, 규모의 기업 선정
- 가상 인턴십 제도에 대한 충분한 이해 업체 선정
- 대상업체 의사소통 관리 위한 전담 Facilitator 지정
- 보안컨설팅 전문컨설턴트 면담 및 간담회 개최 지원



현장중심 보안컨설팅 역량 강화 !!
정보보안 컨설턴트 양성 실습체계 마련!!

현장 중심 실습교육을 통한 보안실무전문가 육성 !!
중소기업 보안진단으로 BoB의 대외인지도 제고 !!

현장 지향형 실습



- 보안컨설팅 인턴십 도입
- 현장 지향형 보안 컨설턴트 양성

이론과 실습 병행체제



- 보안이론 교육과 실습의 병행
- 컨설팅 실습 상황 직접 경험

중소 기업 보안이슈 사전 차단



- 중소기업 보안 취약점 도출
- 보안 이슈에 대한 사전 차단

“프로젝트 핵심성공 요소 ”

멘토링에 대한 이해

실습대상 업체선정

멘토의 전문성

전담 운영 인원배치

BoB 멘토링 환경에 최적화된,
“가상 보안 컨설팅
인턴십 실습 시나리오 개발”

전략 1.

체계적인 실습 커리큘럼

전략 1.

신뢰성 있는 대상기업 선정

전략 1.

BoB 멘토단을 강사로 구성

전략 1.

전담 인력의 프로젝트 관리

Phase. 1

BoB기반 교육 진행 일정계획(2013.11~12)

학습내용	세부 내용
보안컨설팅 Diary 작성	<ul style="list-style-type: none"> - 보안컨설팅에 대한 Framework를 제시하는 노트 - 수행내용에 대한 기록 및 개인별 학습내용을 기록, 지속활용
사전지식 교재 및 교육	<ol style="list-style-type: none"> 1. 보안 컨설팅의 이해(2H) 2. 보안컨설팅 방법론 적용(2H) 3. 보안현황 As-Is 분석기법(2H) 4. 보안대응 To-Be 컨설팅 기법(2H)
문서작성 및 PT역량 강화 교육	<ol style="list-style-type: none"> 1. 컨설팅 결과에 대한 고객과의 커뮤니케이션 역량 향상 2. 프리젠테이션 역량 강화 위한 교육
PT(프리젠테이션) 경진대회	<ol style="list-style-type: none"> 1. PT 경진대회 기획안 작성 2. PT 경진대회 진행 및 심사 3. PT 경진대회 입상자 수상

사전지식 습득위한 커리큘럼 구성으로 정보 보안컨설팅의 기반지식 습득 체계 확립

Phase. 2

BoB기반 실습교육 진행 일정계획(2014.1~2)

학습내용	세부 내용
보안 컨설팅 대상 중소기업 섭외	<ul style="list-style-type: none"> - 사전 보안컨설팅 지원 신청기업으로 구성, 참여도 증대 구현 - 보안 컨설팅 실습에 적합한 다양한 업종, 규모의 기업제시 - 기업 시스템 활용을 위한 네트워크 장비 운영업체 - 기업 업무를 위한 IT시스템 운영 업체
보안컨설팅 수행 인터뷰 및 현장조사	<ul style="list-style-type: none"> - 대상업체 담당자 인터뷰, 자료 요청 등에 대한 업체와의 전달 Facilitator 지정, 역할 수행(1인 비상주)
보안컨설팅 보고회	<ul style="list-style-type: none"> - 착수보고회, 완료보고회 진행
완료보고 산출물 제출	<ul style="list-style-type: none"> - 보안컨설팅에 대한 완료보고회 산출물 인쇄 및 배포
대외기관 홍보	<ul style="list-style-type: none"> - BoB보안컨설팅 인턴쉽 프로젝트의 성공효과 등 대외홍보 지원
보안컨설팅 전문업체 벤치마킹	<ul style="list-style-type: none"> - 보안컨설팅 전문업체 방문 또는 보안컨설팅트와의 간담회 개최

실제 중소기업의 보안컨설팅 수행으로 실무 및 현장 지향형 인재육성 지원



전담 보안컨설팅 인턴쉽 Facilitator 지원(2013.11~2014.02)



프로젝트 성공위한 삼자간 전담 인력배치로 상호 지원 협력 체계 확립

감사합니다.

