Cybersecurity Resiliency for Defense Contractors Webinar Series:
Cybersecurity Compliance – Real Company Examples

October 29, 2020
Jana White

ALPINE SECURITY IMEC

1

Today's Topics

- How to write policies and procedures – and how are they different?
- What to do and what not to do when working towards compliance
- Examples from manufacturers of what works – and what does not

ALPINE SECURITY IMEC

2

ALPINE SECURITY

Service-Disabled Veteran Owned Small Business (SDVOSB)

Areas of Focus:

Cybersecurity Training

Penetration Testing

Vulnerability Assessments

CISO-as-a-Service

Cybersecurity Strategy

DFARS 252.204-7012 & CMMC

Based in Greater St. Louis Area

IMEC

3

What are policies and procedures – and how are they different?

Policies are guidelines or rules that cover **what** an organization expects from employees, and **why**. Policies cover any laws or regulations that apply to your organization and try to ensure compliance with those requirements. **Effective policies set the tone for a healthy work culture.**

Procedures provide step-by-step instructions for specific routine tasks, and to explain **how** things are done. They may include a checklist or process steps for your employees to follow. **Effective procedures ensure that employees know what to do and keep your organization running smoothly.**

ALPINE SECURITY

IMEC

4

How to write policies– The Do List

- Use clear, concise, and simple language
- Explain the rule, not how to implement the rule **(what)**
- Always make it easily accessible to staff
- Cite applicable rules, regulations, or laws and the penalties for non-compliance **(why)**
- **Review at least annually! (document review details)**

ALPINE SECURITY

IMEC

5

How to write policies– The Don't List

- Avoid mixing procedures with policies. Unless a law changes and organization's policy should not require a lot of changes policies (procedures can change frequently)
- Don't use individual's names in the policy, unless you must list out a current team/group like CIRT (Use position titles instead)
- Don't forget to state in each policy that violations of the policy (compliance is not optional)

ALPINE SECURITY

IMEC

6

How to write procedures – The Do List

- Use clear, concise, and simple language
- Address **how** to implement policies
- Always take user experience into account (never make assumptions)
- Include all steps, from start to finish
- Make sure that everyone who does a specific task has access to the procedures for that task
- **Review at least annually! (document review details)**

ALPINE SECURITY

IMEC

7

How to write procedures – The Don't List

- Don't be unnecessarily restrictive or complicated
- Don't skip steps
- Don't forget to determine who is responsible for reviewing, approving, and implementing the procedure (responsible for updates too!)
- Procedures constantly evolve over time, don't forget to document and track version changes!

ALPINE SECURITY

IMEC

8

Common policy examples

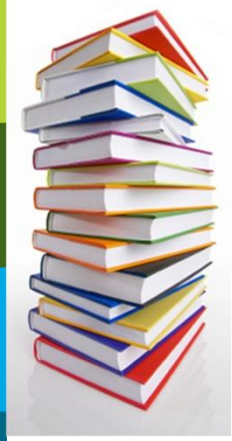
- Acceptable Use Policy
- Clean Desk Policy
- Email Policy
- Password Protection Policy
- Social Engineering/Security Awareness Policy

ALPINE SECURITY

IMEC

9

NIST 800-171 policies you need



- Access control policy
- Auditing, monitoring, logging, & reporting policy
- Configuration management policy
- Identification and authentication policy
- Incident response policy
- Media protection and disposal policy
- Personnel security policy
- Physical security policy
- Security awareness training policy
- System and communications protection policy
- System and information integrity policy
- System maintenance policy
- Risk management policy
- Security assessment and authorization policy

ALPINE SECURITY

IMEC

10

Common procedure examples

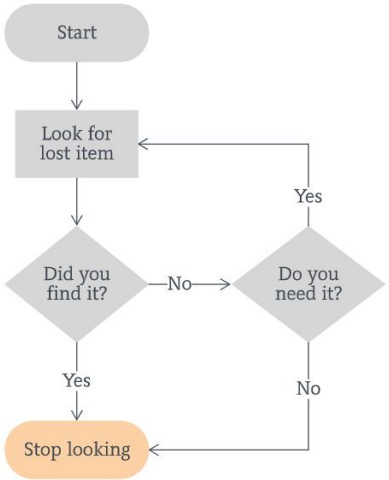
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Incident Response Plan (IRP)
- Standard Operating Procedures (SOP)

ALPINE SECURITY

IMEC

11

Workflow diagram example

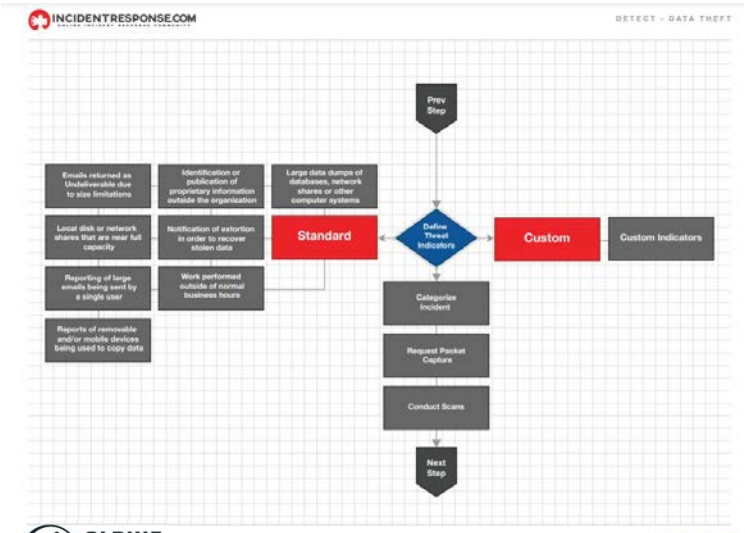


ALPINE SECURITY

IMEC

12

IRP playbook page example



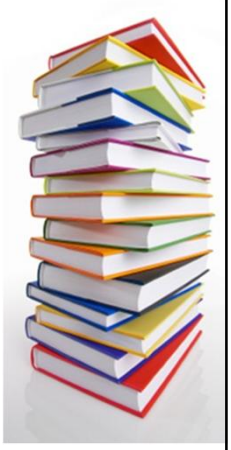
ALPINE SECURITY

IMEC

13

NIST 800-171 procedures you need

- Access control procedures
- Auditing, monitoring, logging, & reporting procedures
- Configuration management procedures
- Identification and authentication procedures
- Incident response procedures (IRP)
- Media protection and disposal procedures
- Personnel security procedures
- Physical security procedures
- Security awareness training procedures
- System and communications protection procedures
- System and information integrity procedures
- System maintenance procedures
- Risk management procedures
- Security assessment and authorization procedures



ALPINE SECURITY

IMEC

14

Compliance 101

The term compliance describes the ability to act according to an order, set of rules, or request.

- Business compliance operates at two levels:
  - *Level 1 - compliance with the external rules that are imposed upon an organization as a whole*
  - *Level 2 - compliance with internal systems of control that are imposed to achieve compliance with the externally imposed rules*

ICA INTERNATIONAL COMPLIANCE ASSOCIATION

ALPINE SECURITY

IMEC

15

Compliance vs. Security

Compliance	Security
Compliance means ensuring an organization meets the minimum requirements of the policies, regulations, and laws that apply to that organization	Security is a clear set of technical systems, tools, and processes put in place to protect and defend the information, personnel, and technology assets of an organization

ALPINE SECURITY

IMEC

16

Why companies should have GRC

GRC (governance, risk, and compliance) — is an umbrella term for the processes and practices that organizations implement to meet business objectives

- *Helps with monitoring and mitigating risks*
- *Helps track regulatory changes and verifies compliance*
- *Aligns policies and processes to organizational goals*

ALPINE SECURITY

IMEC

17

GRC resource example - TiGRIS

TalaTek Intelligent Governance and Risk Integrated Solution (TiGRIS)

The Only FedRAMP-Authorized GRC

Simplify GRC with the TalaTek intelligent Governance and Risk Integrated Solution (TiGRIS) managed service. TiGRIS combines our client-tested SaaS solution with our proven methodology and GRC experts in a single integrated offering. The result is a governance, risk, and compliance program that delivers the comprehensive visibility and control you need to make better informed risk decisions with far less investment than traditional technology-only approaches.

CERBERUS SENTINEL

ALPINE SECURITY

IMEC

18

What to do and what not to do when working towards compliance

- Start with a plan, and then get started!
- Communicate the plan and the progress often
- Focus on continuous improvement
- Set goals and milestones
- Enforce accountability
- Don't forget to explain the "why"
- Don't forget to double check (or triple check) your work

ALPINE SECURITY

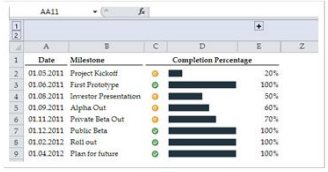
IMEC

19

Make a checklist – Keep it updated!

Use a checklist to keep track of tasks that need to be done, policies and procedures that need to be written, and any processes that need to be developed

- *Use a GANTT style chart with milestones to stay on track*
- *Don't forget about training personnel on new policies, procedures, and practices!*



	Date	Milestone	Completion Percentage
2	01.05.2011	Project Kickoff	20%
3	01.06.2011	First Prototype	100%
4	01.08.2011	Investor Presentation	50%
5	01.09.2011	Alpha Out	60%
6	01.11.2011	Private Beta Out	70%
7	01.12.2011	Public Beta	100%
8	01.02.2012	Roll out	100%
9	01.04.2012	Plan for future	100%

ALPINE SECURITY

IMEC

20

Have a change management process

- Define the change
- Select the change management team
- Identify management sponsorship and secure commitment
- Develop implementation plan including metrics
- Implement the change—in stages, if possible
- Collect and analyze data
- Quantify gaps and understand resistance
- Modify the plan as needed and loop back to the implementation step

ALPINE SECURITY

IMEC

21

Make policies accessible to everyone

Your employees should not have to go through dangers untold and hardships unnumbered just to find your policies.

ALPINE SECURITY

IMEC

22

Provide training for procedures

- Focus on both the how and the why within the procedures
- Explain expectations from a high level, gradually moving to a personal level for the greatest context
- Don't rush the learning process, check often for understanding
- Incorporate hands-on learning as soon as possible
- Develop a training plan and regularly review to identify areas for improvement

ALPINE SECURITY

IMEC

23

Check often for understanding

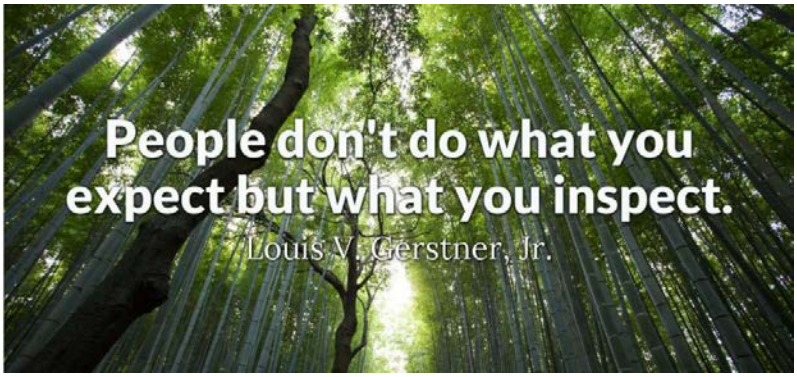
- Don’t assume employees have read or understood your policies, even if they sign off on it!
- The writer’s intention and the reader’s interpretation of a policy may be different
- Ensure knowledge is **current** for existing and/or updated policies
- Have employees show you where a specific policy is located. If they cannot, your policies are not accessible enough

ALPINE SECURITY

IMEC

24

Enforce compliance



ALPINE SECURITY

IMEC

25

Examples from manufacturers of what works – and what does not

What works

- Plan to execute, then execute the plan
- Be prepared for challenges
- Focus on the end goal
- Have accountability buddies (battle buddy)

What does not work

- Delegate and forget
- Waiting until the deadline is on top of you
- Ad hoc implementation
- Lack of support structure from management

ALPINE SECURITY

IMEC

26

Divide and conquer

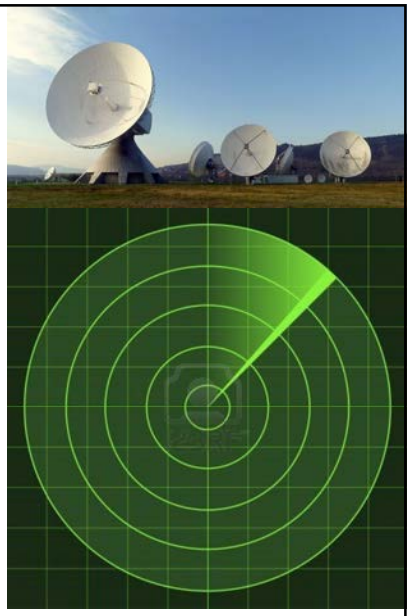
- Divide policy and procedure writing tasks among your team
  - *Use areas of expertise or responsibility*
  - *Peer review draft work*
- Check in on progress frequently
  - *Load balance as needed*
  - *Recognize team efforts*

ALPINE SECURITY

IMEC

27

Keep it on the radar



- **Build a timeline**, always keep the end date in sight
- **Set up weekly or bi-weekly progress updates** with entire team
- Have a project manager **review POAM weekly**
- **Address obstacles or challenges quickly**, don't let it throw off your groove!

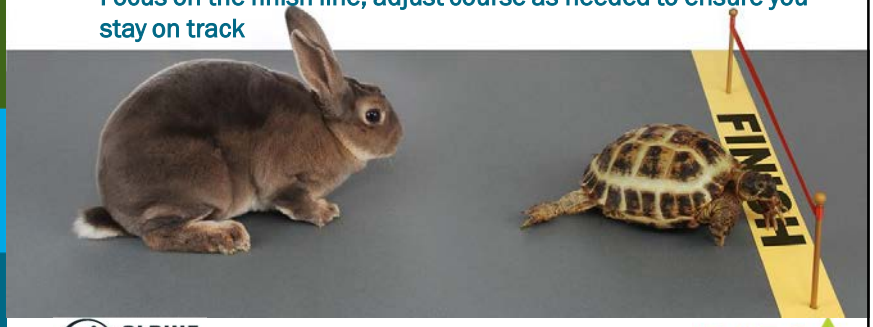
ALPINE SECURITY

IMEC

28

It's ok to be a tortoise! Slow and steady progress wins

- Use your POAM (Plan of Actions and Milestones)
- Complete one task daily
- Have weekly goals/milestones
- Ask for help if you need it
- Focus on the finish line, adjust course as needed to ensure you stay on track



ALPINE SECURITY IMEC

29

Real examples of success with DFARS

RECENT PROJECT IN PARTNERSHIP WITH IMEC

- Rockford area manufacturer
- Company has been in business since 1990
- Proudly supports a global customer base, including more than 60 airlines
- Integral part of the DoD supply chain
- Needed to determine current DFARS NIST 800-171 compliance

ALPINE SECURITY IMEC

30

Management support is critical

- The President took an active role in the project from the very beginning
- Attended team interviews and weekly meetings
- Reviewed and advised on documentation created by his team
- Continues to support the DFARS 800-171 compliance initiative with goal to fully implement all 110 controls by end of year

ALPINE SECURITY

IMEC

31

Commitment and teamwork equals success

- Covid-19 hit U.S. right after the project kicked off
- Client had to rapidly pivot, there were some challenges to overcome
- Never lost sight of the end goal, continued to shrink their CUI information system to a very manageable size
- Had tremendous support from IMEC

ALPINE SECURITY

IMEC

32

Keep your eye on the prize

- Compliance is a big advantage over competitors
- Becoming compliant strengthens the entire U.S. DoD supply chain
- The costs of compliance are less than the cost of a breach
- Security builds brand loyalty, inside and out!

ALPINE SECURITY

IMEC

33

Other Helpful Resources (Freebies!)

- Security Policy Templates - https://www.sans.org/information-security-policy/
- Policy and/or Framework Templates - https://flank.org/
- Incident Response Playbooks - https://www.incidentresponse.com/playbooks/

ALPINE SECURITY

IMEC

34

What We Covered Today…

- How to write policies and procedures – and how are they different?
- What to do and what not to do when working towards compliance
- Examples from manufacturers of what works – and what does not

ALPINE SECURITY

IMEC

35

Jana White
jana.white@alpinesecurity.com
www.alpinesecurity.com
info@alpinesecurity.com
(844) 925-7463

ALPINE SECURITY

IMEC

36