June 19, 2018 | Issue 1

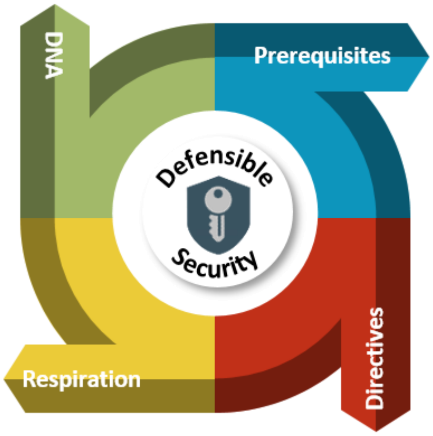
OCIO | Office of the Chief Information Officer

British Columbia

TOPIC: Introduction to Defensible Security

Congratulations on your subscription for the Defensible Security Newsletter. Over the next 12 months, you will receive biweekly newsletters covering control elements of the Defensible Security framework.

Defensible Security (DefSec) helps organizations know what they need to be doing at a minimum to achieve a security posture that is defensible.
It also helps them understand how to do it in a very iterative, pragmatic way.
The DefSec framework is classified in to 4 categories (Prerequisites, Directives Respiration, and DNA) which make up the 25 control elements of the framework.



"Covering the organization end-to-end"

Controls in the Security Prerequisites category ensure the importance of cybersecurity is recognized by executives in the organization. It also ensures that

An organization is defensible when they are at or above compliance. However, hygiene and compliance level controls should be fully functional within the organization prior to pursuing or achieving a risk-based or world-class security posture.

World-Class Level
At this level, security controls within the organization change as technology and risk changes. Essentially the organization implements next-generation security controls. An organization is truly at this level when they have progressed from compliance and risk-based levels, while ensuring continuous hygiene practices. Additionally, they take a world-class approach to mitigating security risk which usually involves using cutting-edge technology.

Risk-Based Level
At this level, the organization takes a risk-based approach in protecting its information assets. Security controls are implemented based on security threats and risk assessments, and the controls are sufficient to mitigate risks to an acceptable level.

Compliance Level
At this level, controls are implemented based on compliance requirements. For the BC government, it includes (but is not limited to) the following compliance documents:

- Core Policy and Procedures Manual
- Information Security Policy
- Human Resource Policy

Hygiene Level
This level is a health check of the organization, it is ensuring the basics are being done to protect information assets. Obtaining "Green" in all controls at this level doesn't necessarily mean the organization is secure, but means that the organization's security posture at this level is optimal. We find that 50% of attacks (including ransomware and phishing) occur at this level.

roles and responsibilities are identified, risks are documented and reviewed, and security and risk assessments are conducted. Some of the controls in this category include:

- **Risk Appetite and Register**
- **Crown Jewels**

Controls in the Security Directives category outline authoritative controls, ensuring the tone at the top is translated into policies and procedures, and plans are in place to ensure smooth business operation. Some of the controls in this category include:

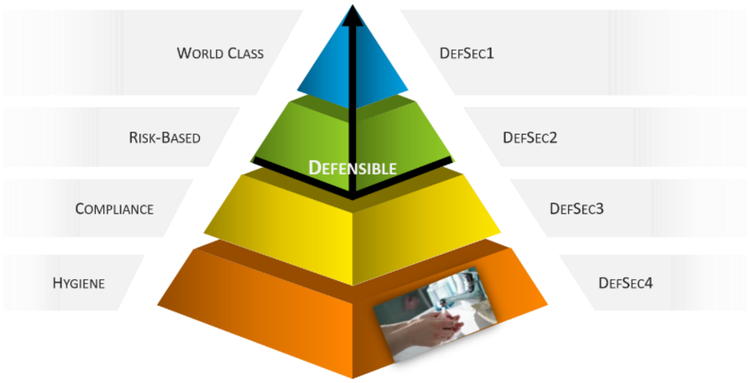
- **Information Security Policy**
- **Change Management**
- **Incident Management**
- **Business Continuity Plan**
- **Disaster Recovery Plan**

Controls in the Security Respiration category are operative controls which assist in embedding security into the practices of the organization. Some of the controls in this category include:

- **Backup and Retention**
- **Logging and Monitoring**
- **Logical and Physical Access**
- **Personnel Security**

Controls in the Security DNA category ensure security is embedded into the culture of the organization. Some of the controls in this category include:

- **Information Classification**
- **Security Awareness Program**



The newsletters you will be receiving will focus on the Hygiene level of the DefSec Security posture pyramid.

KEY EVENTS

- **Monthly Defensible Security Conference Call: July 2018**
  This month's conference call will cover introduction to DefSec and the first control element (Executive Support) of the DefSec framework.

- **BC Security Day: Nov 7, 2018**
  The Province organizes and hosts two "Security Day" events each year (Spring and Fall), free of charge. Representatives from the broader public sector, school districts, post secondary institutions, municipalities, and crown corporations are encouraged to attend. Visit the Security Day website for more information.

- **20th Privacy and Security Conference: Feb 2019**
  Held in Victoria, British Columbia, Canada this conference is a must attend. This three-day conference, is recognized as one of the top tier events in North America. Anyone working in the information privacy and security fields will benefit from the speakers, discussions, and networking at the conference. The conference draws an international audience of some 1,000 delegates with an interest in cutting edge policy, programs, law, research, and technologies aimed at the protection of privacy and security.