

# Measuring the Maturity of your Security Operations Center?

## **The Perfect Score May Surprise You**



New report finds global IT security lacking undermined by over-reliance on technology.

Few organizations today have reached optimal security maturity.

#### HP found that

## **3 out of 4**

organizations are unable to achieve basic consistency of operations.

## **Only 30%**

of organizations that formally define business goals and compliance requirements are able to meet them.

On the path to maturity, it's possible to try too hard and become rigid. Level 5 is not the goal.

#### Security operations maturity model and methodology

Researchers at HP have developed the SOMM model to evaluate enterprise security maturity. Companies with no security operations capability score 0. A tightly controlled, continually measured, and ever-evolving capability scores 5. The optimal score for most organizations is not 5, since costs can outweigh the benefits. Instead, companies should aim for 3.

SOMM Level	Rating	Description
Level O	Incomplete	Operational elements <b>do</b> <b>not exist</b> .
Level 1	Initial	<b>Minimum requirements</b> are met without standardization, documentation or repeatability.
Level 2	Managed	<b>Baseline business goals are</b> <b>met</b> with task documentation, enabling any staff member to perform and modify reactively.
Level 3	Defined	<b>Operations are well-defined</b> , subjectively evaluated, and flexible with proactive modifications. This is the ideal maturity level for most enterprise SOCs.
Level 4	Measured	Operations are qualitatively evaluated, reviewed, and proactively improved using business and performance metrics. This is the ideal maturity level for most managed service provider SOCs.
Level 5	Optimizing	<b>Processes are rigid</b> and continually measured for deficiency and variation within a tightly controlled environment, requiring significant overhead.

**Source:** HP Enterprise Security

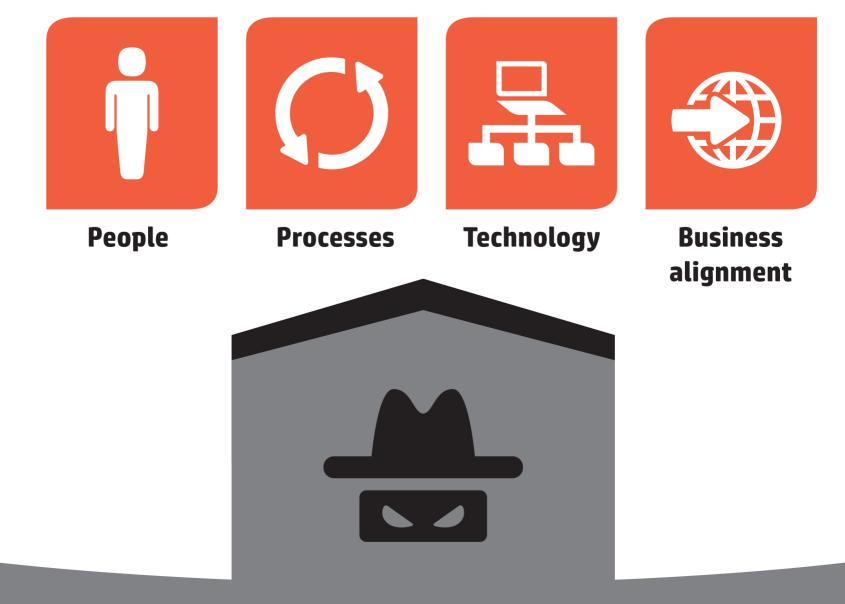


## Why Not Drive to 5?

By level 5, analyst procedures are often overly detailed, including exhaustive screen shots and flow charts—details that limit the quality and speed of response. The costly impact on time and resources associated with Level 5 SOCs outweigh potential benefits.

Focus on continual evolution required to achieve and maintain maturity.

Regardless of what stage you are at, HP can help you enact new best practices that align with the primary criteria of SOC maturity:



### When Cyber Crime Strikes

Getting breached is the fastest way to bring focus to your security maturity. Don't be caught off guard or tempted to rush post-breach into a quick fix. Create a solid foundation which will allow you to quickly address high-priority improvements.

Read the full report on **"2014 State of Security Operations"** at **hp.com/go/StateOfSecOps** 

Learn how HP can help you on the path to SOC maturity at **hp.com/go/sioc** 

