



# DoubleCheck CYBERSECURITY RISK MANAGEMENT

- 👍 **Cybersecurity Risk is More Than IT Risk**
- 👍 **NIST Cybersecurity Framework Offers Guidance**
- 👍 **Where Does Your Organization Stand?**

IT security – aka cybersecurity – is of key interest and importance to virtually every enterprise. It doesn't take much imagination to understand the implications of a breach – customer data can be damaged, destroyed or made public; key business information may be similarly compromised; systems can be hijacked for nefarious purposes – all of which can have a serious negative impact on your firm's operations, public image and finances. How well does your firm understand its Cybersecurity Risks?

## Highlights

NIST (the National Institute of Standards and Technology – part of the U.S. Department of Commerce) has developed a well-accepted (voluntary) cybersecurity framework, including standards, guidelines and best practices to manage cybersecurity risk.



Based on the NIST standards, DoubleCheck enables your firm to develop a Framework Profile, which presents cybersecurity outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories.



The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.



Your Profiles will be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).



## Key Benefits

- ✔ The DoubleCheck CSRM will compare your company's controls to the NIST controls, and determine if there are other CyberSecurity controls that your firm should be considering, or controls that you should consider removing or modifying.
- ✔ The DoubleCheck CSRM Profile provides an alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.
- ✔ Ultimately, this profiling process and associated action plans typically results in affirming, modifying and/or creating a family of business processes, controls and testing procedures tailored to the specifics of the enterprise and reflective of the threats it faces.
- ✔ The tools support the processes, data elements, and analytics that enable you to deliver a well-managed, well-understood, organizationally engaged cybersecurity risk management program
- ✔ Results are delivered in board-ready, pixel-perfect reports that will provide insights to your Cybersecurity Risk Management.





# Questions that will get answered with Doublecheck's Cybersecurity Risk Management



Do we have a current, complete inventory of IT resources, with the data in each system well categorized?



Do we have a good inventory of all significant known threats and risks to our IT resources?



Do we have a good set of controls in place, assuring our IT resources are well protected against risks and threats, and consider both mitigation (prevention) and remediation (event response)?



Do we have evidence to believe the answers to these questions? In other words, are our controls "good" enough, appropriately covering the threats and risks?



Has the design of our controls been reviewed by subject matter experts?



Are the controls appropriately tested to see if they truly work as designed?

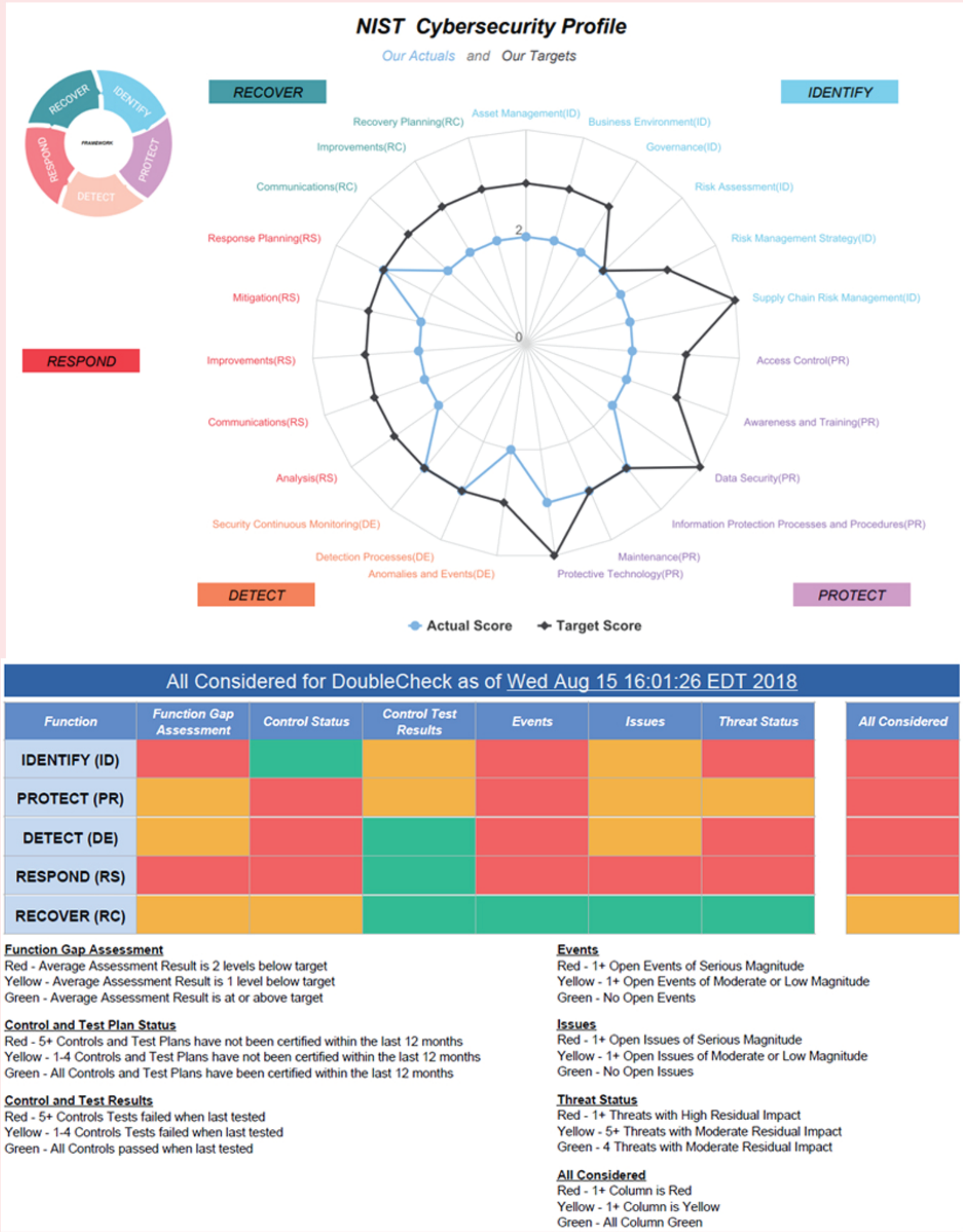


Have the control designs and test plans been appropriately reviewed? Are all controls being tested in the "right places" at the right frequency?



Have we had any events that would suggest we need to update our controls?

Of course, key to program effectiveness is communication – clearly and effectively sharing results and trends, demonstrating the firm has a robust cybersecurity program, based on standards, with appropriate formality of process and clear accountability for results. Shown below are examples of reports that help involved parties understand the firm's cybersecurity status.



## ABOUT DOUBLECHECK

DoubleCheck™ LLC is a leading enterprise-level governance, risk management, compliance and audit solutions software company. The DoubleCheck GRC and audit platform can automate and unify on a single platform any or all of any organization's governance, risk management, compliance and testing (GRC and audit) activities. This includes key requirements such as Sarbanes-Oxley compliance, corporate governance, risk and audit management. The solution is highly configurable, offering adaptations to easily fit each client's needs.